

PAUL ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
AUSTIN MANES (State Bar No. 284065)
amanes@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiff
FINJAN, INC.

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

FINJAN, INC., a Delaware Corporation,
Plaintiff,
v.
CHECK POINT SOFTWARE
TECHNOLOGIES INC., a Delaware
Corporation, CHECK POINT SOFTWARE
TECHNOLOGIES LTD., an Israeli Limited
Company,
Defendants.

Case No.:

COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. (“Finjan”) files this Complaint for Patent Infringement and Demand for Jury Trial against Check Point Software Technologies Ltd. (“Check Point Israel”) and Check Point Software Technologies, Inc. (“Check Point USA”) (collectively, “Defendant” or “Check Point”) and alleges as follows:

THE PARTIES

1. Finjan is a Delaware Corporation with its principal place of business at 2000 University Avenue, Suite 600, E. Palo Alto, California 94303.

2. Check Point USA is a Delaware Corporation with its headquarters and principal place of business at 959 Skyway Road, Suite 300, San Carlos, CA 94070. Defendant may be served through its agent for service of process, Corporation Service Company, 2710 Gateway Oaks Drive, Suite 150N, Sacramento, CA 95833.

3. Check Point Israel is limited company organized under the law of Israel with its headquarters and principal place of business at 5 Ha'Solelim Street, Tel Aviv 67897, Israel. On information and belief, Check Point USA is a wholly-owned subsidiary of Check Point Israel.

JURISDICTION AND VENUE

4. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq.* This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

5. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and/or 1400(b).
Venue is proper at least because Check Point's U.S. Headquarters is located in this District at 959
Skyway Road Suite 300, San Carlos, CA 94070.

6. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant regularly and continuously does business in this District and has infringed or induced infringement, and continues to do so, in this District. Upon information and belief, Check Point's U.S. Headquarters is located in this District in the city of San Carlos, California and is a regular and established place of business. In fact, Defendant's website regularly advertises active job listings in this District for its U.S. Headquarters in this District. *See Exhibit 1 attached hereto*

1 (https://careers.checkpoint.com/careers/index.php?m=careers&a=jobs&country_code=US). As such,
2 the Court has personal jurisdiction over Check Point because minimum contacts have been
3 established within this forum and the exercise of jurisdiction would not offend traditional notions of
4 fair play and substantial justice.

5 **INTRADISTRICT ASSIGNMENT**

6 7. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district-
7 wide basis.

8 **FINJAN'S INNOVATIONS**

9 8. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an
10 Israeli corporation. In 1998, Finjan moved its headquarters to San Jose, California. Finjan was a
11 pioneer in developing proactive security technologies capable of detecting previously unknown and
12 emerging online security threats, recognized today under the umbrella term "malware." These
13 technologies protect networks and endpoints by identifying suspicious patterns and behaviors of
14 content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous
15 patents covering innovations in the United States and around the world resulting directly from
16 Finjan's more than decades-long research and development efforts, supported by a dozen inventors
17 and over \$65 million in R&D investments.

18 9. Finjan built and sold software, including application program interfaces (APIs) and
19 appliances for network security, using these patented technologies. These products and related
20 customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed
21 nearly 150 employees around the world building and selling security products and operating the
22 Malicious Code Research Center, through which it frequently published research regarding network
23 security and current threats on the Internet. Finjan's pioneering approach to online security drew
24 equity investments from two major software and technology companies, the first in 2005 followed by
25 the second in 2006. Finjan generated millions of dollars in product sales and related services and
26 support revenues through 2009, when it spun off certain hardware and technology assets in a merger.
27 Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under
28

1 which it could not make or sell a competing product or disclose the existence of the non-compete
 2 clause. Finjan became a publicly traded company in June 2013, capitalized with \$30 million. After
 3 Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015,
 4 Finjan re-entered the development and production sector of secure mobile products for the consumer
 5 market.

6 **FINJAN'S ASSERTED PATENTS**

7 10. On November 28, 2000, U.S. Patent No. 6,154,844 ("the '844 Patent"), titled SYSTEM
 8 AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A
 9 DOWNLOADABLE, was issued to Shlomo Touboul and Nachshon Gal. A true and correct copy of
 10 the '844 Patent is attached to this Complaint as Exhibit 2 and is incorporated by reference herein.

11 11. All rights, title, and interest in the '844 Patent have been assigned to Finjan, who is the
 12 sole owner of the '844 Patent. Finjan has been the sole owner of the '844 Patent since its issuance.

13 12. The '844 Patent is generally directed toward computer networks, and more particularly,
 14 provides a system that protects devices connected to the Internet from undesirable operations from
 15 web-based content. One of the ways this is accomplished is by linking a security profile to such web-
 16 based content to facilitate the protection of computers and networks from malicious web-based
 17 content.

18 13. On November 15, 2005, U.S. Patent No. 6,965,968 ("the '968 Patent"), entitled
 19 POLICY-BASED CACHING, was issued to Shlomo Touboul. A true and correct copy of the '968
 20 Patent is attached to this Complaint as Exhibit 3 and is incorporated by reference herein.

21 14. All rights, title, and interest in the '968 Patent have been assigned to Finjan, who is the
 22 sole owner of the '968 Patent. Finjan has been the sole owner of the '968 Patent since its issuance.

23 15. The '968 Patent is generally directed towards methods and systems for enabling policy-
 24 based cache management to determine if digital content is allowable relative to a policy. One of the
 25 ways this is accomplished is scanning digital content to derive a content profile and determining
 26 whether the digital content is allowable for a policy based on the content profile.

1 16. On August 26, 2008, U.S. Patent No. 7,418,731 (“the ‘731 Patent”), entitled METHOD
2 AND SYSTEM FOR CACHING AT SECURE GATEWAYS, was issued to Shlomo Touboul. A true
3 and correct copy of the ‘731 Patent is attached to this Complaint as Exhibit 4 and is incorporated by
4 reference herein.

5 17. All rights, title, and interest in the ‘731 Patent have been assigned to Finjan, who is the
6 sole owner of the ‘731 Patent. Finjan has been the sole owner of the ‘731 Patent since its issuance.

7 18. The ‘731 Patent is generally directed towards methods and systems for providing an
8 efficient security system. One of the ways this is accomplished is by implementing a variety of caches
9 to increase performance of the system.

10 19. On January 12, 2010, U.S. Patent No. 7,647,633 (“the ‘633 Patent”), entitled
11 MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued
12 to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll and Shlomo Touboul. A true and
13 correct copy of the ‘633 Patent is attached to this Complaint as Exhibit 5 and is incorporated by
14 reference herein.

15 20. All rights, title, and interest in the ‘633 Patent have been assigned to Finjan, who is the
16 sole owner of the ‘633 Patent. Finjan has been the sole owner of the ‘633 Patent since its issuance.

17 21. The ‘633 Patent is generally directed towards computer networks, and more
18 particularly, provides a system that protects devices connected to the Internet from undesirable web-
19 based content. One of the ways this is accomplished is by determining whether any part of such web-
20 based content can be executed and then trapping such content using mobile protection code.

21 22. On December 13, 2011, U.S. Patent No. 8,079,086 (“the ‘086 Patent”), entitled
22 MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued
23 to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R Kroll and Shlomo Touboul. A true and
24 correct copy of the ‘086 Patent is attached to this Complaint as Exhibit 6 and is incorporated herein.

25 23. All rights, title, and interest in the ‘086 Patent have been assigned to Finjan, who is the
26 sole owner of the ‘086 Patent. Finjan has been the sole owner of the ‘086 Patent since its issuance.

1 24. The ‘086 Patent is generally directed towards computer networks and, more
 2 particularly, provides a system that protects devices connected to the Internet from undesirable
 3 operations from web-based content. One of the ways this is accomplished is by creating a profile of
 4 the web-based content and sending a representation of these profiles to another computer for
 5 appropriate action.

6 25. On March 20, 2012, U.S. Patent No. 8,141,154 (“the ‘154 Patent”), titled SYSTEM
 7 AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was
 8 issued to David Gruzman and Yuval Ben-Itzhak. A true and correct copy of the ‘154 Patent is attached
 9 to this Complaint as Exhibit 7 and is incorporated by reference herein.

10 26. All rights, title, and interest in the ‘154 Patent have been assigned to Finjan, who is the
 11 sole owner of the ‘154 Patent. Finjan has been the sole owner of the ‘154 Patent since its issuance.

12 27. The ‘154 Patent is generally directed toward a gateway computer protecting a client
 13 computer from dynamically generated malicious content. One of the ways this is accomplished is by
 14 using a content processor to process a first function and invoke a second function if a security
 15 computer indicates that it is safe to invoke the second function.

16 28. On March 18, 2014, U.S. Patent No. 8,677,494 (“the ‘494 Patent”), titled
 17 MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued
 18 to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul. A true and
 19 correct copy of the ‘494 Patent is attached to this Complaint as Exhibit 8 and is incorporated by
 20 reference herein.

21 29. All rights, title, and interest in the ‘494 Patent have been assigned to Finjan, who is the
 22 sole owner of the ‘494 Patent. Finjan has been the sole owner of the ‘494 Patent since its issuance.

23 30. The ‘494 Patent is generally directed toward a method and system for deriving security
 24 profiles and storing the security profiles. One of the ways this is accomplished is by deriving a
 25 security profile for a downloadable, which includes a list of suspicious computer operations, and
 26 storing the security profile in a database.

31. The ‘844 Patent, the ‘968 Patent, the ‘731 Patent, the ‘633 Patent, the ‘154 Patent, the ‘086 Patent, and the ‘494 Patent, as described above, are collectively referred to as the “Asserted Patents” herein.

FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANT

32. Check Point has long been aware of Finjan and its proprietary technology. For example, on January 28, 1997, Finjan and Check Point partnered in providing solutions for Java Security. Finjan issued a press release describing the partnership with Check Point that involved integrating Finjan's proprietary scanning technology into Check Point's firewalls. A true and correct copy of the press release is attached to this Complaint as Exhibit 9. In its 1999 Annual Report, Check Point listed Finjan as a "Framework Partner." A true and correct copy of the Check Point 1999 Annual Report is attached to this Complaint as Exhibit 10. Furthermore, on February 27, 2001, Finjan and Check Point entered into a Partner Exhibitor Agreement for Trade Shows.

33. Finjan reached out to Check Point as early as 2014 to discuss Check Point licensing of Finjan's patents related to its behavior-based and anti-malware security technology. On December 8, 2016, Finjan sent notice of the Asserted Patents in a letter addressed to Gil Schwed, the Chief Executive Officer of Check Point. A true and correct copy of the letter is attached to this Complaint as Exhibit 11. The letter notified Check Point that it was offering both products and services that infringe patents owned by Finjan. The letter included an appendix providing the patent numbers of the '844 Patent, '968 Patent, '731 Patent, '633 Patent, '086 Patent, and '494 Patent and the relevant Check Point Products. The letter also included a link to a page on Finjan's website that listed Finjan's entire patent portfolio.

34. On February 9, 2017, Finjan called Check Point about the December 8, 2016, letter and spoke with a Check Point representative. Finjan sent a follow-up email on December 8, 2016 letter to memorialize the conversation. Finjan received no response to its call or email. Finjan again contacted Check Point via email or other form of electronic messaging on July 31, 2017; September 28, 2017; November 6, 2017; and February 21, 2018. Finjan received no responses from Check Point regarding these inquiries.

1 **CHECK POINT'S PRODUCTS AND TECHNOLOGIES**

2 35. Defendant makes, uses, sells, offers for sale, and/or imports into the United States and
 3 this District the following products and services: Check Point's Next Generation Firewall and
 4 Security Gateway products, Blade products, CloudGuard products, Endpoint Protection products,
 5 Advanced Threat Prevention products, Mobile Security products, ZoneAlarm products, Threat
 6 Intelligence products, Security Management and Policy Management products, ThreatCloud
 7 Managed Security Service products, Smart-1 Appliance products, products using SandBlast
 8 technology, and products utilizing the Gaia Operating System.

9 **CHECK POINT'S NEXT GENERATION FIREWALL AND SECURITY GATEWAY**
 10 **PRODUCTS**

11 36. Check Point's Next Generation Firewalls provide data and network security protection
 12 in an integrated firewall and gateway platform. Check Point offers Next Generation Firewalls and
 13 Security Gateways for Cloud, Data Center, Midsized and Enterprise, Small Business, Consumer, and
 14 Home Office. Next Generation Firewalls and Security Gateways operate as gateways that provide
 15 all-inclusive security from cyber threats with Check Point Threat Prevention and integration with
 16 Check Point's SandBlast technology.

17 **ALL-INCLUSIVE SECURITY**



18 THREAT PREVENTION



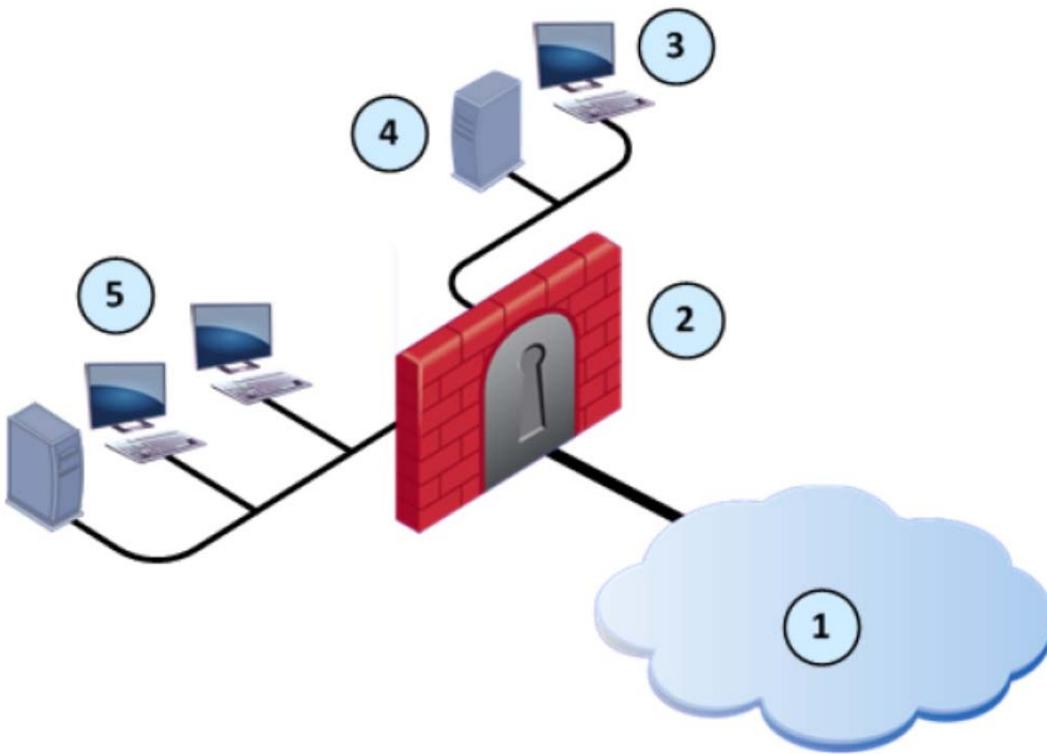
19 THREAT PREVENTION + SANDBLAST

20 Exhibit 12 at 6.

21 37. Check Point's Next Generation Firewalls and Security Gateways allow the
 22 enforcement of security policies that serve as a collection of rules to control network traffic and
 23 enforce organization guidelines for data protection and access to resources. The Next Generation
 24 Firewalls and Security Gateways include the ThreatSpect Engine for multi-tiered analysis of network
 25

1 traffic and correlation of data across multiple layers, including through antivirus, reputation, and
 2 behavioral patterns.

3 **Components of the Check Point Solution**



17 Exhibit 13 at Page 14.

18 38. Check Point's Next Generation Firewalls and Security Gateways include different
 19 packages, including the NGTP with Antivirus, Anti-Bot, and email security and NGTX with the
 20 NGTP protection and SandBlast technology.

21 **ALL-INCLUSIVE SECURITY SOLUTIONS**

22 Check Point 5900 Next Generation Security Gateways offer a
 23 complete and consolidated security solution available in two
 24 complete packages:

- 25 • NGTP: prevent sophisticated cyber-threats with
 Application Control, URL Filtering, IPS, Antivirus,
 Anti-Bot and Email Security.
- 26 • NGTX: NGTP with SandBlast Zero-Day Protection,
 which includes Threat Emulation and Threat
 Extraction.

1 39. Check Point's Next Generation Firewalls and Security Gateways are available as both
2 hardware appliances and virtual appliances. Next Generation Firewalls and Security Gateways
3 include unified malware and bot protection, which records extensive forensics regarding the detected
4 malware and associated events.

Unified Malware and Bot Protection

The Antivirus Software Blade is unified with the Anti-Bot Software Blade to give both pre-and post-infection protection to organizations and provide multi-layered threat prevention. Administrators can manage unified policies and reports all in a single user interface.



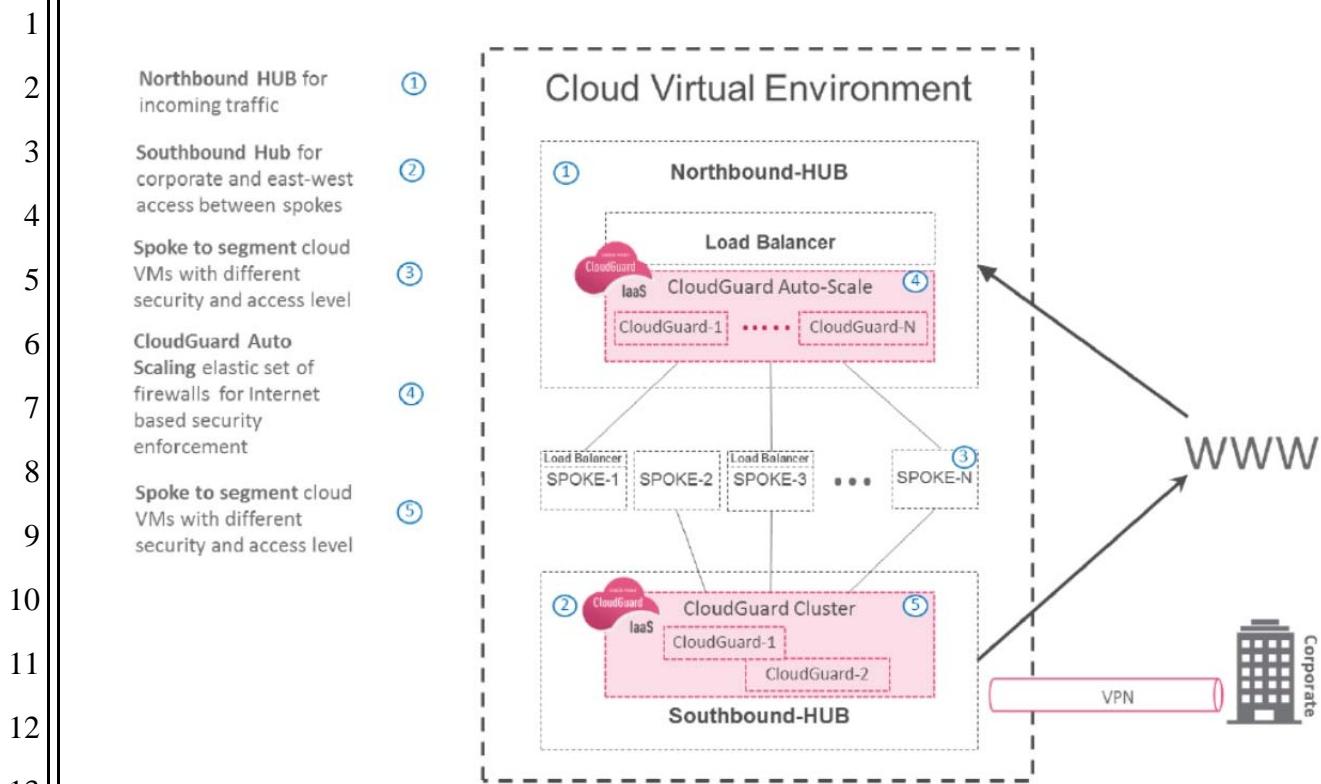
Extensive Forensics.

Exhibit 14 at Page 2.

CHECK POINT'S CLOUDGUARD PRODUCTS

40. Check Point's CloudGuard products offer zero-day threat protection, identity protection, and data protection and are offered for Security as a Service ("SaaS") and Infrastructure as a Service ("IaaS") for public and private clouds. CloudGuard provides threat prevention security through shared intelligence and advanced threat prevention technology. CloudGuard SaaS provides advanced security and threat prevent for SaaS applications. CloudGuard IaaS provides advanced threat prevention for public and private cloud platforms like Amazon Web Services, Google Cloud Platform, Microsoft Azure, Cisco ACI, OpenStack, VMware NSX, VMware Cloud on AWS, VMware ESX, Alibaba Cloud, KVM, and Hyper-V.

41. CloudGuard employs a hub and spoke model to provide security policy enforcement on network traffic.



14 Exhibit 15 at 6.

ENDPOINT PROTECTION PRODUCTS

15
16 42. Check Point's Endpoint Protection products protect endpoints from attacks and zero-day threats through antivirus, anti-bot, and threat prevention. Endpoint Protection monitors,
17 manages, and enforces user security policies on an endpoint.
18

19
20
21
22
23
24
25
26
27
28

AUTOMATIC TRIGGERS	
1	• Anti-Bot detection on the network or on the endpoint
2	• Threat Emulation detection on the network
3	• Check Point Antivirus detection on the endpoint
4	• Third-party Antivirus detection on the endpoint
5	• Manual Indicators of Compromise (IoCs)
DAMAGE DETECTION	
6	• Automatically identify: Data exfiltration, data manipulation or encryption, key logging
ROOT CAUSE ANALYSIS	
8	• Trace and identify root cause across multiple system restarts in real-time
MALWARE FLOW ANALYSIS	
10	• Automatically generates interactive graphic model of the attack flow
MALICIOUS BEHAVIOR DETECTION	
12	• Over 40 malicious behavior categories
13	• Hundreds of malicious indicators

Exhibit 16 at 3.

43. Endpoint Protection allows endpoint security to be unified on a single management console and applied with a straightforward policy language.

CHECK POINT'S ADVANCED THREAT PREVENTION PRODUCTS AND SANDBLAST

44. Check Point's Advanced Threat Prevention products provide zero-day protection for networks and detect evasion-resistant malware. Advanced Threat Prevention products include SandBlast Technology for threat emulation, threat extraction, and practical prevention. Advanced Network Threat Prevention is offered for Network, Endpoint, and Mobile, and is directly and indirectly used by Check Point products.

45. Advanced Threat Prevention for Network Security provides an evasion resistant sandbox to catch unknown malware, eliminate threats, and deliver safe files to users. Advanced Threat Prevention for Network Security products include "SandBlast" technology to provide zero-day protection through Threat Emulation and Threat Extraction for next level detection of evasive

1 malware. SandBlast can be used in a number of different implementations, including as an appliance,
 2 as an agent, through a distributed deployment, as SandBlast service, inline or span-port deployment,
 3 mail transfer agent (MTA), or through a Threat Prevent API. SandBlast Threat Emulation performs
 4 deep level inspection of downloaded content, including both executables and data files, before the
 5 malware has a chance to deploy. SandBlast Threat Emulation runs downloaded files in a virtual
 6 sandbox to discover malicious behavior by monitoring the instructions performed and determining if
 7 the instruction relate to an exploit from malware. SandBlast Threat Emulation includes CPU-Level
 8 Inspection, which looks into the execution flow to determine if an exploitation method was used.
 9 SandBlast Threat Emulation creates a detailed report for each file that is emulated and found to be
 10 malicious. SandBlast Threat Extraction extracts potentially malicious content, such as macros or
 11 embedded links, from files to allow prompt delivery of clean and reconstructed versions of these files
 12 that only include known safe elements. SandBlast automatically shares newly discovered attack
 13 information with ThreatCloud.

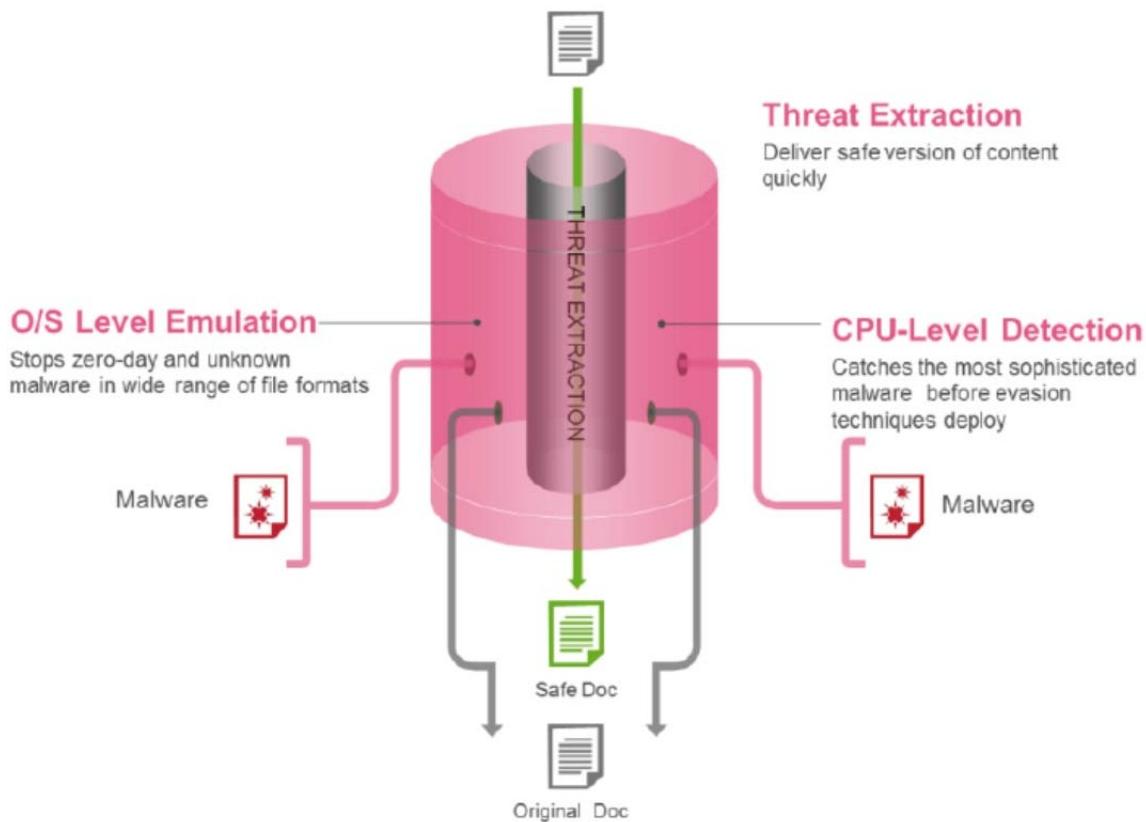


Exhibit 17 at 2 (August 2, 2016).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The screenshot shows a 'Malware Report' interface. At the top left, there's a file icon and the text 'sample.xls'. To its right, a red warning icon with the text 'Malicious Activity Detected'. Below this, there are details about the file: Type (xls), File Size (546.3 KB), MD5 (5f9b7a70cad65a54ff8879ab10ff6edde), and SHA1 (b3e7b78086725d3be76a2a447886bcace218194a). A link 'Download malicious file' is present. To the right of the file details is an 'Emulation Screenshot' showing a computer monitor with a blue screen. On the right side of the report, there are two vertical panels: 'Prevention / ...' and 'Session' statistics.

Malware Report

Emulated On:

sample.xls

Malicious Activity Detected

Type: xls
File Size: 546.3 KB
MD5: 5f9b7a70cad65a54ff8879ab10ff6edde
SHA1: b3e7b78086725d3be76a2a447886bcace218194a

[Download malicious file](#)

Emulation Screenshot

0 Suspicious Activities

6 Affected Processes

6 Processes Created | 3 Processes Terminated | 0 Processes Crashed

C:\Documents and Settings\...\Local Settings\Temp\dcs.tmp
C:\Program Files\Microsoft Office\OFFICE11\EXCELEXE
C:\Program Files\Windows NT\dhcphost.exe
C:\WINDOWS\system32\attrib.exe
more

1 Affected Registry Keys

4 Affected Files

3 Files Created | 3 Files Modified | 2 Files Deleted

Prevention / ...

Session

68
55
15
10
10
n

HUNT Session

28
28
28
28
20

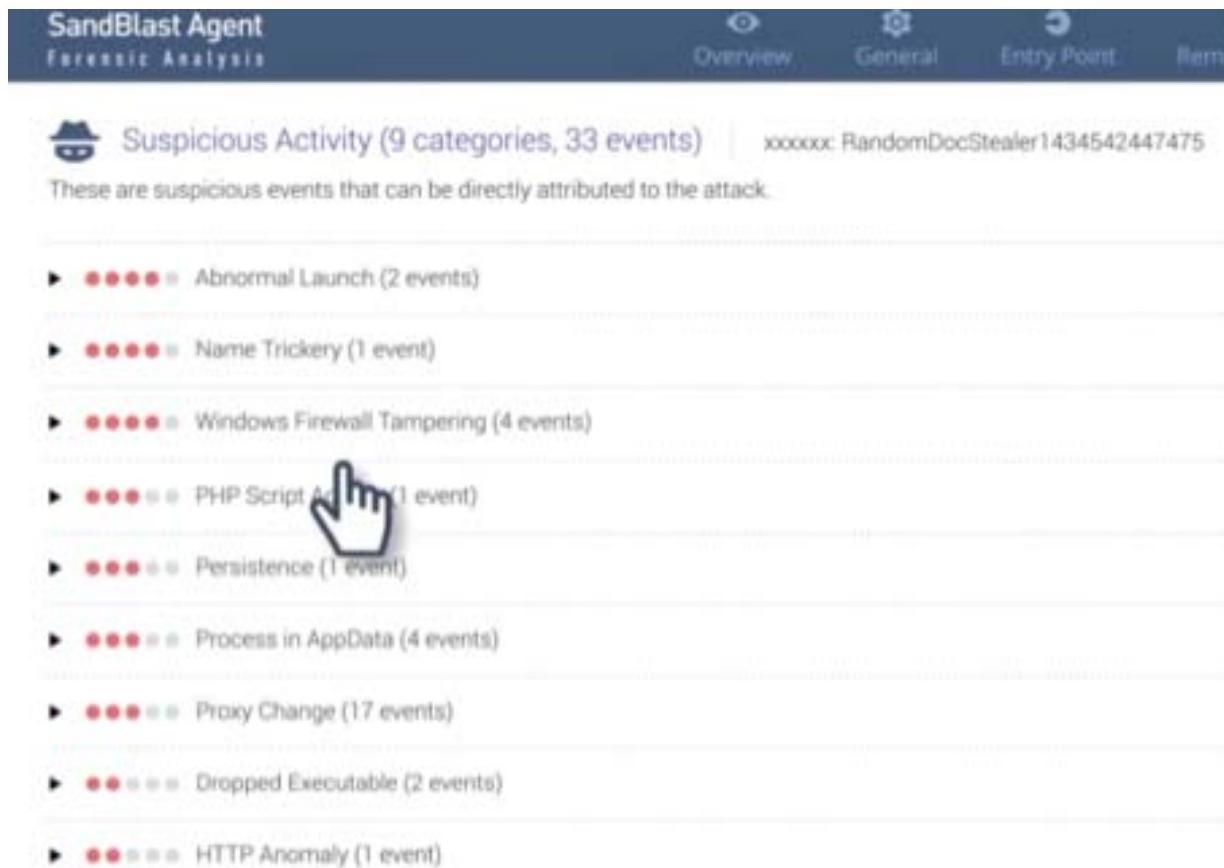
a report for each emulated environment shows suspicious activities and includes screenshots

Exhibit 23.



Exhibit 24.

1 46. Advanced Threat Prevention for Endpoint Protection provides SandBlast agents and
 2 browser extensions that prevent evasive attacks based on unknown and zero-day malware, intercept
 3 these attacks at runtime using behavioral analysis and forensic insights, and contain and remediate
 4 the harmful impact of these attacks. SandBlast Agents collect and store suspicious activity on a
 5 computer and provides a rating indicating the level of suspiciousness associated with that activity.



The screenshot shows a software interface titled "SandBlast Agent" and "Forensic Analysis". At the top, there are tabs for "Overview", "General", "Entry Point", and "Removal". The main area is titled "Suspicious Activity (9 categories, 33 events)". It displays a list of suspicious events with icons and counts:

- ▶ Abnormal Launch (2 events)
- ▶ Name Trickery (1 event)
- ▶ Windows Firewall Tampering (4 events)
- ▶ PHP Script Analysis (1 event) 
- ▶ Persistence (1 event)
- ▶ Process in AppData (4 events)
- ▶ Proxy Change (17 events)
- ▶ Dropped Executable (2 events)
- ▶ HTTP Anomaly (1 event)

21 Exhibit 22.

22 47. Check Point's Advanced Threat Prevention for Mobile Threat Prevention protects
 23 mobile devices from infected apps, man-in-the-middle attacks over Wi-Fi, OS Exploits, and
 24 malicious links. Mobile Advanced Threat Prevention applies threat emulation, advanced static code
 25 analysis, app reputation, and machine learning. Advanced Threat Prevention for Mobile Threat
 26 Defense utilizes SandBlast for detecting whether a device is secure.

1 **ZONEALARM PRODUCTS**

2 48. Check Point's ZoneAlarm products are a suite of products that offers security features
3 like behavioral antivirus, threat emulation, advanced firewall, identify protection, and protection from
4 ransomware. ZoneAlarm allows users to send downloaded files like email attachments to a virtual
5 cloud-based sandbox that will emulate the files and analyze the resulting behavior. ZoneAlarm also
6 comes with advanced browser protects against websites for dangerous scripts, files, and other
7 executables before they are downloaded onto the user's computer, thereby preventing scrips or files
8 from saving to disk or executing.

9 **THREAT INTELLIGENCE PRODUCTS**

10 49. Check Point's Threat Intelligence includes ThreatCloud IntelliStore, Incident
11 Response Service, Managed Security Service, and Private ThreatCloud. Threat Intelligence uses
12 evidence-based knowledge like context, mechanisms, indicators, implications and actionable advice
13 about an existing or emerging menace and is used to inform decisions regarding response to the
14 menace.

15 50. ThreatCloud IntelliStore provides organizations with real-time threat intelligence.
16 ThreatCloud IntelligenceStore provides access to a wide range of protection, but also allows the
17 picking and choosing of threat intelligence feeds based on a company's unique needs (by geography,
18 industry, or threat type). ThreatCloud Intelligence store creates a robust set of security protections
19 and updates security gateways.

20
21
22
23
24
25
26
27
28



Exhibit 18 at Page 3.

CHECK POINT'S THREATCLOUD PRODUCTS

51. Check Point's ThreatCloud performs automated analysis to find significant events on a network. Check Point ThreatCloud uses these events to identify malicious activity. ThreatCloud delivers real-time dynamic threat intelligence to security gateways to identify and stop emerging threats.

SERVICE LEVEL AGREEMENTS (SLA)			
The following table summarizes ThreatCloud Managed Security Services SLAs for the three service levels offered.			
	Standard	Premium	Elite
Description	Threat Prevention Monitoring and Alerting Service	Expert Assisted Threat Prevention and Alerting Service	Full Threat Prevention Management Service
Blades supported	IPS, Anti-Bot, Antivirus, URL Filtering, Application Control, & Threat Emulation	IPS, Anti-Bot, Antivirus, URL Filtering, Application Control, & Threat Emulation	IPS, Anti-Bot, Antivirus, URL Filtering, Application Control, & Threat Emulation

Exhibit 19 at 2.

CHECK POINT'S SECURITY MANAGEMENT PRODUCTS

52. Check Point's Security Management Products (which include Smart-1 Appliances) manage growing networks, disruptive technologies, and the proliferation of interconnected devices demand a new approach to managing security. Check Point's Security Management Products operate as a single management solution to centrally correlate all types of events across all network environment, cloud services, and mobile infrastructures.

1 UNIFIED, INTELLIGENT SECURITY MANAGEMENT



Exhibit 12 at Page 14.

53. Check Point's Infinity technology provides consolidated security and threat prevention across networks, cloud, and mobile. Check Point Infinity includes R80.10, which merges technology into an easy to use console that provides full spectrum visibility.

10 MAIN COMPONENTS OF THE R80.10 SECURITY MANAGEMENT SOLUTION

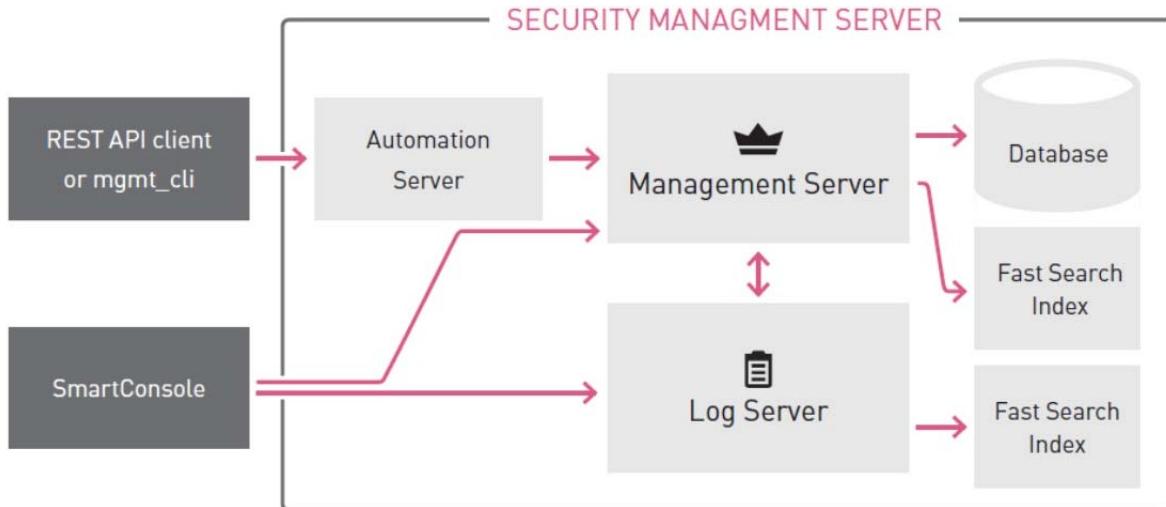


Exhibit 20 at Page 3.

20 DEFENDANT'S INFRINGEMENT OF FINJAN'S PATENTS

54. Defendant has been and is now infringing, and will continue to infringe, the Asserted Patents in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale its Check Point's Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products, Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products, ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management products, ThreatCloud

1 Managed Security Service products, Smart-1 Appliance products, products using SandBlast
2 technology, and products utilizing the Gaia Operating System. (“Accused Products”).

3 55. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a),
4 either literally or under the doctrine of equivalents, or both, Defendant indirectly infringes all the
5 Asserted Patents by instructing, directing, and/or requiring others, including its customers,
6 purchasers, users, and developers, to perform all or some of the steps of the method claims, either
7 literally or under the doctrine of equivalents, or both, of the Asserted Patents.

COUNT I

(Direct Infringement of the ‘844 Patent pursuant to 35 U.S.C. § 271(a))

10 56. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
11 allegations of the preceding paragraphs, as set forth above.

23 58. The ‘844 Accused Products embody the patented invention of the ‘844 Patent and
24 infringe the ‘844 Patent because they practice a method of receiving by an inspector a downloadable,
25 generating by the inspector first downloadable security profile that identifies suspicious code in the
26 received downloadable, and linking by the inspector the first downloadable security profile to the
27 downloadable before a web server makes the downloadable available to web clients. *See generally*

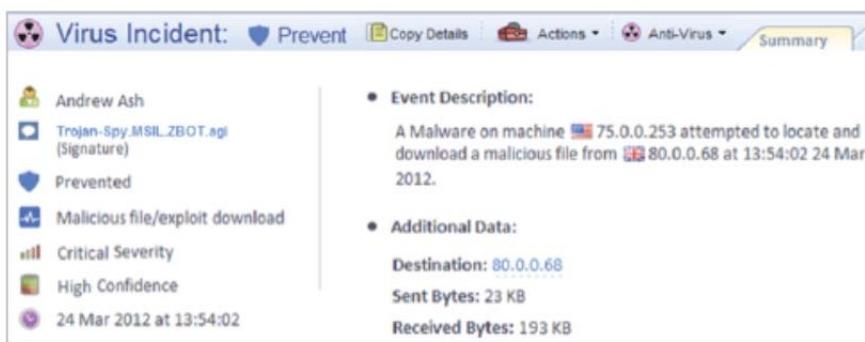
1 Exhibit 2. For example, as shown below, the ‘844 Accused Products provide gateway security to end
 2 users, where incoming downloadables (e.g., PDFs with JavaScript, EXE files, or JavaScript embedded
 3 within an HTML file) are received by the ‘844 Products.

4 59. For example, the ‘844 Accused Products include emulation technology that uses an
 5 evasion resistant sandbox to catch unknown downloaded malware and eliminates threats and delivers
 6 safe files to users. The ‘844 Accused Products create a report with detailed information identifying
 7 suspicious code that was present in the content. The ‘844 Accused Products link the generated
 8 information on suspicious code before a web server make the content available to a web client that
 9 requested the content.

10 60. For example, the ‘844 Accused Products perform extensive forensics regarding the
 11 detected malware and associated events to identify suspicious code.

12 **Unified Malware and Bot Protection**

13 The Antivirus Software Blade is unified with the Anti-Bot
 14 Software Blade to give both pre-and post-infection protection
 15 to organizations and provide multi-layered threat prevention.
 Administrators can manage unified policies and reports all in
 a single user interface.



22 Extensive Forensics.

23 Exhibit 14 at Page 2.

24 61. For example, SandBlast Threat Emulation performs deep level inspection of
 25 downloaded content, both executables and data files, before the malware has a chance to deploy.
 SandBlast Threat Emulation runs files in a virtual sandbox to discover malicious behavior by
 26 monitoring the instructions performed and determining if the instruction relate to an exploit from
 27

1 malware. SandBlast Threat Emulation includes CPU-Level Inspection, which looks into the
 2 execution flow to determine if an exploitation method was used. SandBlast Threat Emulation creates
 3 a detailed report that identifies suspicious code for each file that is emulated and found to be
 4 malicious. SandBlast Threat Extraction extracts potentially malicious content, such as macros or
 5 embedded links, from files to allow prompt delivery of clean and reconstructed versions of these files
 6 that only include known safe elements. SandBlast automatically shares newly discovered attack
 7 information with ThreatCloud.

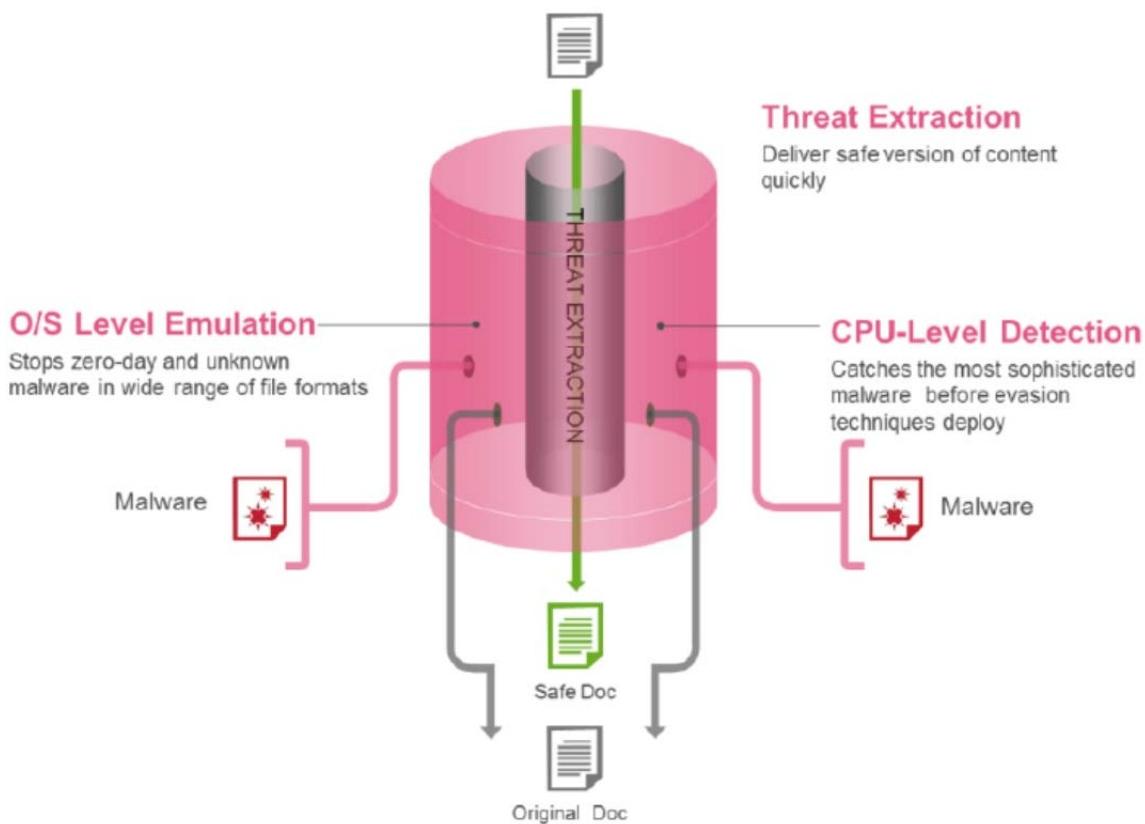




Exhibit 25.

63. For example, suspicious activity is recorded about suspicious code that is detected.

The screenshot shows the SandBlast Agent Forensic Analysis interface. At the top, there's a navigation bar with tabs: Overview, General, Entry Point, and Item. Below the tabs, a section titled "Suspicious Activity (9 categories, 33 events)" is displayed. To the right of this title is a code identifier: "xxxxxx: RandomDocStealer1434542447475". A sub-section below the main title says, "These are suspicious events that can be directly attributed to the attack." A list of nine categories follows, each preceded by a small icon and a descriptive name:

- ▶ Abnormal Launch (2 events)
- ▶ Name Trickery (1 event)
- ▶ Windows Firewall Tampering (4 events)
- ▶ PHP Script Analysis (1 event)
- ▶ Persistence (1 event)
- ▶ Process in AppData (4 events)
- ▶ Proxy Change (17 events)
- ▶ Dropped Executable (2 events)
- ▶ HTTP Anomaly (1 event)

Exhibit 22.

64. Defendant's infringement of the '844 Patent has injured Finjan in an amount to be proven at trial.

65. Defendant has been long-aware of Finjan's patents, including the '844 Patent, and has acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '844 Patent. Defendant has had specific knowledge and notice of its infringement of the '844 Patent since at least in or about December 2016, when Finjan specifically identified and described the following products made, used, or sold by Defendants as infringing the '844 Patent: Threat Prevention Products, products with SandBlast zero-day protection, Next Generation Firewall products, Web Security products, Mobile Security products, and Endpoint Security products.

66. On information and belief, despite its knowledge of the ‘844 Patent and its knowledge of its own infringement of that patent since at least in or about December 2016, Defendant made no effort to design its products or services around the ‘844 Patent in order to avoid infringement. Instead, on information and belief, Defendant incorporated infringing technology into additional products, such as those identified in this Complaint. All of these actions demonstrate Defendant’s blatant and egregious disregard for Finjan’s patent rights.

COUNT II

(Indirect Infringement of the ‘844 Patent pursuant to 35 U.S.C. § 271(b))

67. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

68. Defendant has induced infringement of one or more claims of the ‘844 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the ‘844 Patent, Defendant indirectly infringes the ‘844 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘844 Patent, where all the steps of the method claims are performed by either Defendant or its customers, purchasers, users and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either

1 themselves or in conjunction with Defendant, one or more method claims of the ‘844 Patent,
2 including Claims 1-14 and 23-31.

3 69. Defendant knowingly and actively aided and abetted the direct infringement of the ‘844
4 Patent by instructing and encouraging its customers, purchasers, users and developers to use the ‘844
5 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third
6 parties to use the ‘844 Accused Products in an infringing manner, providing a mechanism through
7 which third parties may infringe the ‘844 Patent, advertising and promoting the use of the ‘844
8 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties
9 on how to use the ‘844 Accused Products in an infringing manner.

10 70. Defendant updates and maintains an website with Defendant's administration guides,
11 user guides, operating instructions, and training and certifications which cover in depth aspects of
12 operating the '844 Accused Products. *See, e.g.*,

13 https://supportcenter.checkpoint.com/supportcenter/portal, attached hereto as Exhibit 21.

COUNT III

(Direct Infringement of the ‘968 Patent pursuant to 35 U.S.C. § 271(a))

16 71. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
17 allegations of the preceding paragraphs, as set forth above.

18 72. Defendant has infringed and continues to infringe Claims 1-38 of the ‘968 Patent in
19 violation of 35 U.S.C. § 271(a). Defendant’s infringement is based upon literal infringement or
20 infringement under the doctrine of equivalents, or both. Defendant’s acts of making, using, importing,
21 selling, and/or offering for sale infringing products and services have been without the permission,
22 consent, authorization, or license of Finjan. Defendant’s infringement includes the manufacture, use,
23 sale, importation and/or offer for sale of Defendant’s products and services, including Check Point’s
24 Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products,
25 Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products,
26 ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management
27 products, ThreatCloud Managed Security Service products, Smart-1 Appliance products, products

1 using SandBlast technology, and products utilizing the Gaia Operating System (collectively, the “‘968
2 Accused Products”).

3 73. The ‘968 Accused Products embody the patented invention of the ‘968 Patent and
4 infringe the ‘968 Patent because they embody a policy-based cache manager with a memory storing a
5 cache of digital content, a plurality of policies, and a policy index to the cache contents, the policy
6 index including entries that relate cache content and policies by indicating cache content that is
7 known to be allowable relative to a given policy, for each of a plurality of policies; a content scanner,
8 communicatively coupled with said memory, for scanning a digital content received, to derive a
9 corresponding content profile; and a content evaluator, communicatively coupled with said memory,
10 for determining whether a given digital content is allowable relative to a given policy, based on the
11 content profile, the results of which are saved as entries in the policy index. *See generally* Exhibit 3.

12 74. For example, as shown below, the ‘968 Accused Products provide gateway security to
13 end users, where incoming digital content (e.g., PDFs with JavaScript, EXE files, or JavaScript
14 embedded within an HTML file) are received by the ‘968 Accused Products. The ‘968 Accused
15 Products includes the Gaia operating system, which allows for applying security models to incoming
16 content to enforce consistent network security. The ‘968 Accused Products include emulation
17 technology that uses an evasion resistant sandbox to scan for unknown downloaded malware and
18 eliminates threats and delivers safe files to users. The ‘968 Accused Products cache the files and
19 create a report with detailed information identifying suspicious code that was present in the content.

20 75. For example, the ‘968 Accused Products include Next Generation Firewalls and
21 Security Gateways with security policies that serve as a collection of rules that control network traffic
22 and enforce organization guidelines for data protection and access to resources. The Next Generation
23 Firewalls and Security Gateways include the ThreatSpect Engine for multi-tiered analysis of network
24 traffic and correlation of data across multiple layers, including through antivirus, reputation, and
25 behavioral patterns.

26
27
28

Components of the Check Point Solution

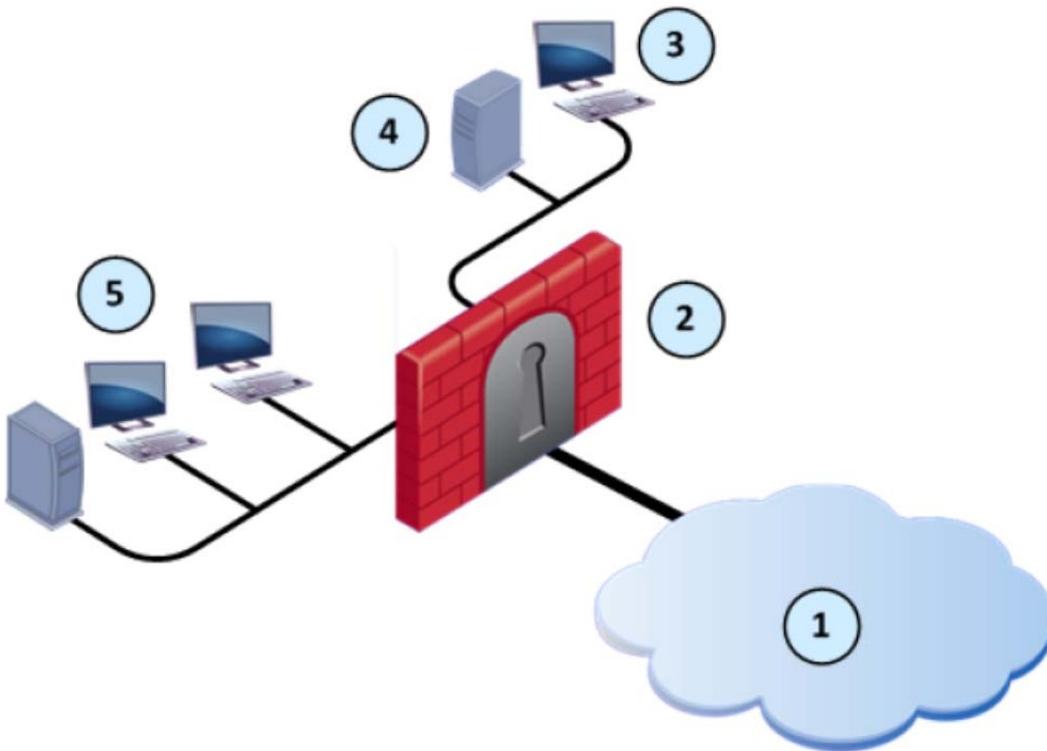


Exhibit 13 at Page 14.

76. For example, the '968 Accused Products include Smart-1 appliances for security policy application.



Exhibit 12 at Page 14.

77. For example, the '968 Accused Products scan content and create content profiles through creation of extensive forensics regarding the detected malware and associated events.

1 **Unified Malware and Bot Protection**

2 The Antivirus Software Blade is unified with the Anti-Bot
 3 Software Blade to give both pre-and post-infection protection
 4 to organizations and provide multi-layered threat prevention.
 5 Administrators can manage unified policies and reports all in
 6 a single user interface.



7 Extensive Forensics.

8 Exhibit 14 at Page 2.

9 78. For example, the ‘968 Accused Products infringe because SandBlast Threat Emulation
 10 scans content and creates content profiles when it performs deep level inspection of downloaded
 11 content, both executables and data files, before the malware has a chance to deploy. SandBlast
 12 Threat Emulation runs files in a virtual sandbox to discover malicious behavior by monitoring the
 13 instructions performed and determining if the instruction relate to an exploit from malware.
 14 SandBlast Threat Emulation includes CPU-Level Inspection, which looks into the execution flow to
 15 determine if an exploitation method was used. SandBlast Threat Emulation creates a detailed report
 16 for each file that is emulated and found to be malicious. SandBlast Threat Extraction extracts
 17 potentially malicious content, such as macros or embedded links, from files to allow prompt delivery
 18 of clean and reconstructed versions of these files that only include known safe elements. SandBlast
 19 automatically shares newly discovered attack information with ThreatCloud.

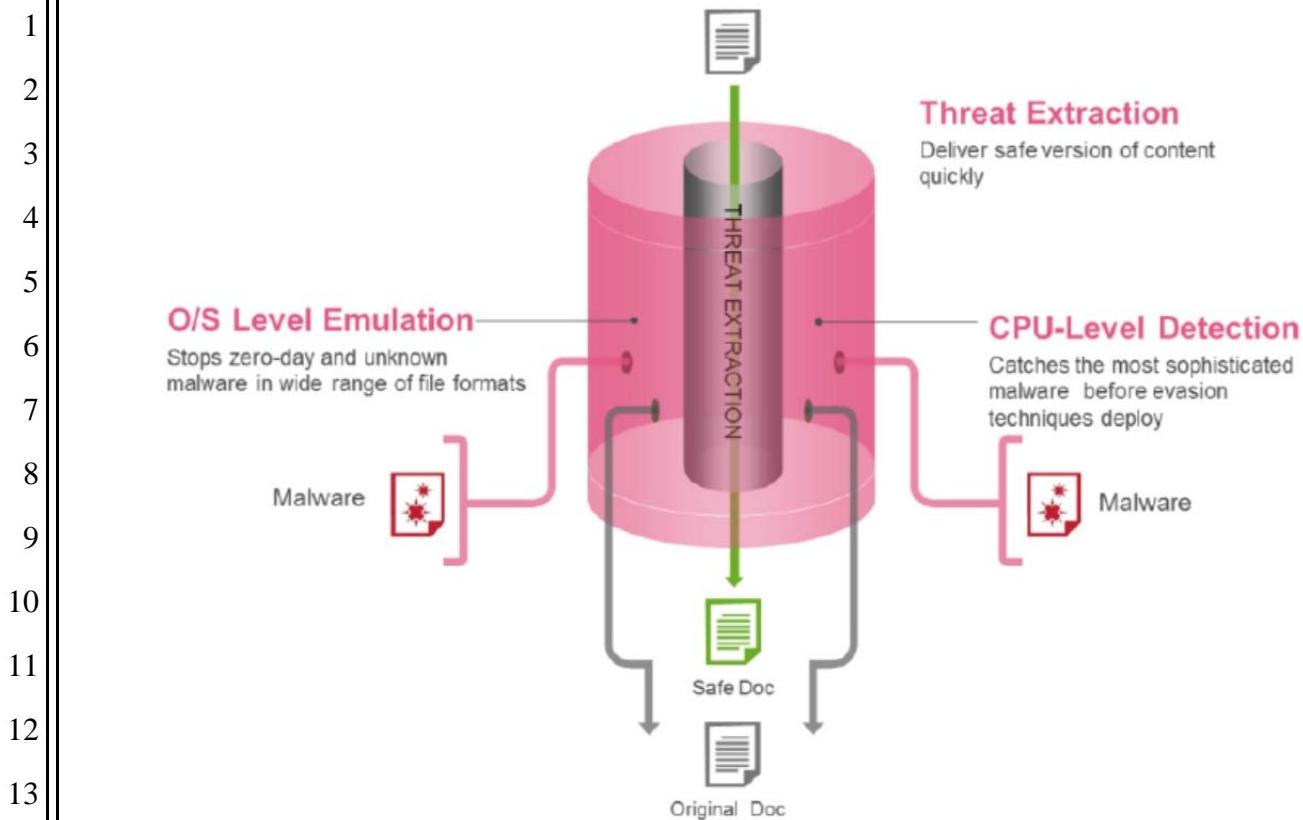


Exhibit 17 at Page 2 (August 2, 2016).

79. For example, the '968 Accused Products determine allowability of content relative to a security policy to performs inline stopping of malicious failed before they reach a web client and shares these results with other systems.



Exhibit 25.

As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant both compete in the security software space, as described above. And Finjan is actively engaged in licensing its patent portfolio, as described above. Check Point's continued infringement of the '968 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

Defendant's infringement of the '968 Patent has injured Finjan in an amount to be proven at trial.

Defendant has been long-aware of Finjan's patents, including the '968 Patent, and has acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '968 Patent. Defendant has had specific knowledge and notice of its infringement of the '968 Patent since at least in or about December 2016, when Finjan specifically

1 identified and described the following products made, used, or sold by Defendants as infringing the
2 '968 Patent: Threat Prevention products, products with SandBlast zero-day protection, Next
3 Generation Firewall products, Web Security products, Mobile Security products, and Endpoint
4 Security products.

5 83. On information and belief, despite its knowledge of the ‘968 Patent and its knowledge
6 of its own infringement of that patent since at least in or about December 2016, Defendant made no
7 effort to design its products or services around the ‘968 Patent in order to avoid infringement.
8 Instead, on information and belief, Defendant incorporated infringing technology into additional
9 products, such as those identified in this Complaint. All of these actions demonstrate Defendant’s
10 blatant and egregious disregard for Finjan’s patent rights.

COUNT IV

(Indirect Infringement of the '968 Patent pursuant to 35 U.S.C. § 271(b))

13 84. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
allegations of the preceding paragraphs, as set forth above.
14

15 85. Defendant has induced and continues to induce infringement of one or more claims of
16 the ‘968 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the ‘968 Patent,
17 Defendant indirectly infringes the ‘968 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing
18 and/or requiring others, including customers, purchasers, users and developers, to perform some of
19 the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘968 Patent,
20 where all the steps of the method claims are performed by either Defendant or its customers,
21 purchasers, users and developers, or some combination thereof. Defendant knew or was willfully
22 blind to the fact that it was inducing others, including customers, purchasers, users and developers, to
23 infringe by practicing, either themselves or in conjunction with Defendant, one or more method
24 claims of the ‘968 Patent, including Claims 13-22 and 25-31.

25 86. Defendant knowingly and actively aided and abetted the direct infringement of the ‘968
26 Patent by instructing and encouraging its customers, purchasers, users and developers to use the ‘968
27 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third

1 parties to use the ‘968 Accused Products in an infringing manner, providing a mechanism through
2 which third parties may infringe the ‘968 Patent, advertising and promoting the use of the ‘968
3 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties
4 on how to use the ‘968 Accused Products in an infringing manner.

5 87. Defendant updates and maintains an website with Defendant's administration guides,
6 user guides, operating instructions, and training and certifications which cover in depth aspects of
7 operating the '968 Accused Products. *See, e.g.*,

<https://supportcenter.checkpoint.com/supportcenter/portal>, attached hereto as Exhibit 21.

COUNT V

(Direct Infringement of the '731 Patent pursuant to 35 U.S.C. § 271(a))

11 88. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
12 allegations of the preceding paragraphs, as set forth above.

13 89. Defendant has infringed and continues to infringe Claims 1-22 of the ‘731 Patent in
14 violation of 35 U.S.C. § 271(a). Defendant’s infringement is based upon literal infringement or
15 infringement under the doctrine of equivalents, or both. Defendant’s acts of making, using, importing,
16 selling, and/or offering for sale infringing products and services have been without the permission,
17 consent, authorization, or license of Finjan. Defendant’s infringement includes the manufacture, use,
18 sale, importation and/or offer for sale of Defendant’s products and services, including Check Point’s
19 Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products,
20 Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products,
21 ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management
22 products, ThreatCloud Managed Security Service products, Smart-1 Appliance products, products
23 using SandBlast technology, and products utilizing the Gaia Operating System (collectively, the “‘731
24 Accused Products”).

25 90. The '731 Accused Products embody the patented invention of the '731 Patent and
26 infringe the '731 Patent because they embody a computer gateway for an intranet of computers, with
- a scanner for scanning incoming files from the Internet and deriving security profiles for the

1 incoming files, wherein each of the security profiles comprises a list of computer commands that a
2 corresponding one of the incoming files is programmed to perform; a file cache for storing files that
3 have been scanned by the scanner for future access, wherein each of the stored files is indexed by a
4 file identifier; and a security profile cache for storing the security profiles derived by the scanner,
5 wherein each of the security profiles is indexed in the security profile cache by a file identifier
6 associated with a corresponding file stored in the file cache; and a security policy cache for storing
7 security policies for intranet computers within the intranet, the security policies each including a list
8 of restrictions for files that are transmitted to a corresponding subset of the intranet computers. *See*
9 *generally* Exhibit 4.

10 91. For example, as shown below, the '731 Accused Products provide gateway security to
11 end users, where incoming files (e.g., PDFs with JavaScript, EXE files, or JavaScript embedded
12 within an HTML file) are received by the '731 Accused Products. The '731 Accused Products
13 include emulation technology that uses an evasion resistant sandbox to scan for unknown downloaded
14 malware and eliminates threats and delivers safe files to users by identifying suspicious computer
15 commands that correspond to the incoming file. The '731 Accused Products cache the files and create
16 a report with detailed information identifying suspicious code that was present in the content. The
17 '731 Accused Products includes the Gaia operating system, which allows to apply policies through a
18 security models to incoming content to enforce consistent network security.

19 92. For example, the '731 Accused Products scan content and create content profiles by
20 applying forensics regarding the detected malware and associated events and computer commands.
21
22
23
24
25
26
27
28

1 **Unified Malware and Bot Protection**

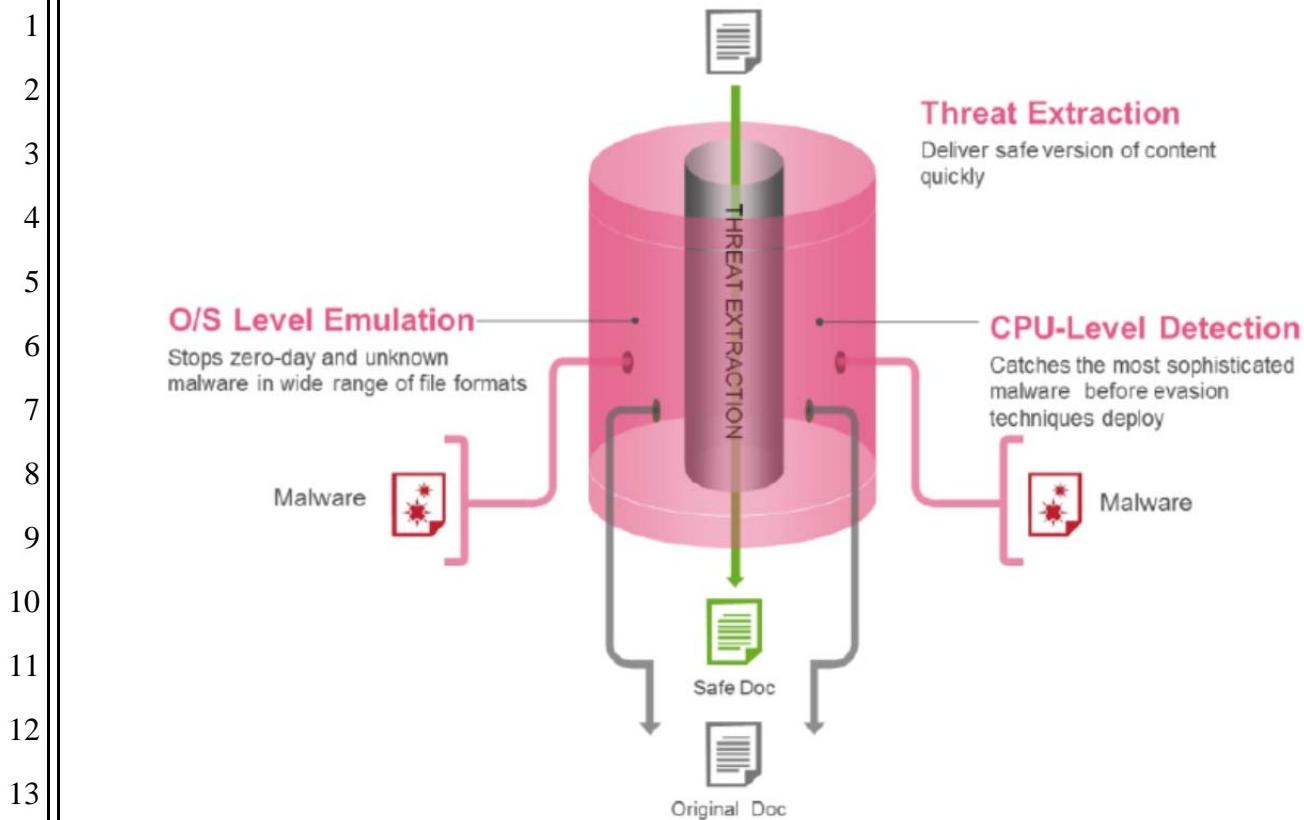
2 The Antivirus Software Blade is unified with the Anti-Bot
 3 Software Blade to give both pre-and post-infection protection
 4 to organizations and provide multi-layered threat prevention.
 5 Administrators can manage unified policies and reports all in
 6 a single user interface.



7 Extensive Forensics.

8
 9
 10
 11 Exhibit 14 at Page 2.

12
 13 93. For example, the '731 Accused Products infringe because SandBlast Threat Emulation
 14 scans content and creates content profiles when it performs deep level inspection of downloaded
 15 content, both executables and data files, before the malware has a chance to deploy. SandBlast
 16 Threat Emulation runs files in a virtual sandbox to discover malicious behavior by monitoring the
 17 instructions and computer commands performed and determining if the instruction relate to an exploit
 18 from malware. SandBlast Threat Emulation includes CPU-Level Inspection, which looks into the
 19 execution flow of computer commands to determine if an exploitation method was used. SandBlast
 20 Threat Emulation creates a detailed report for each file that is emulated and found to be malicious.
 21 SandBlast Threat Extraction extracts potentially malicious content, such as macros or embedded
 22 links, from files to allow prompt delivery of clean and reconstructed versions of these files that only
 23 include known safe elements. SandBlast automatically shares newly discovered attack information
 24 with ThreatCloud.



14 Exhibit 17 at 2 (August 2, 2016).

15 94. For example, the '731 Accused Products determine whether to allow content relative to
16 a security policy indicating restrictions on files transmitted to clients.

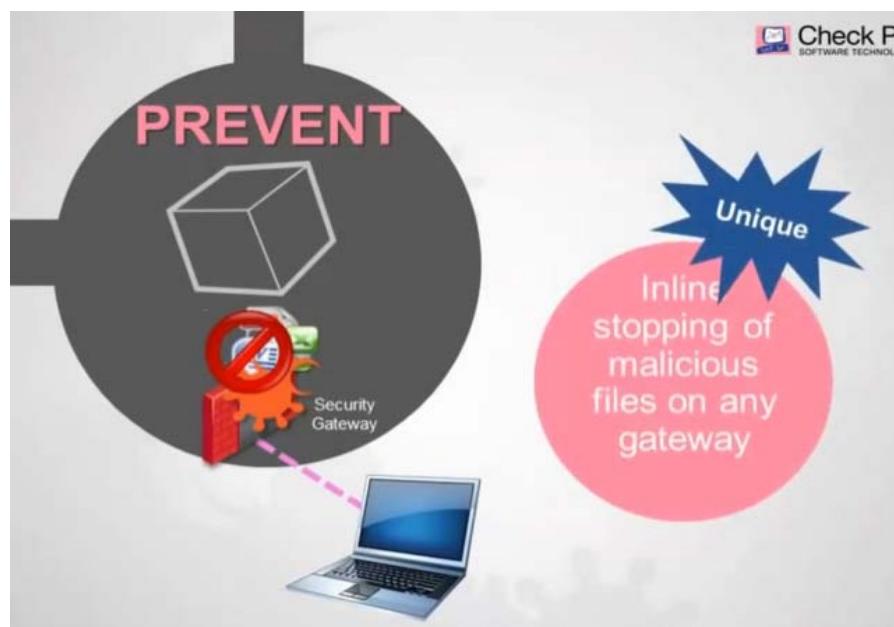
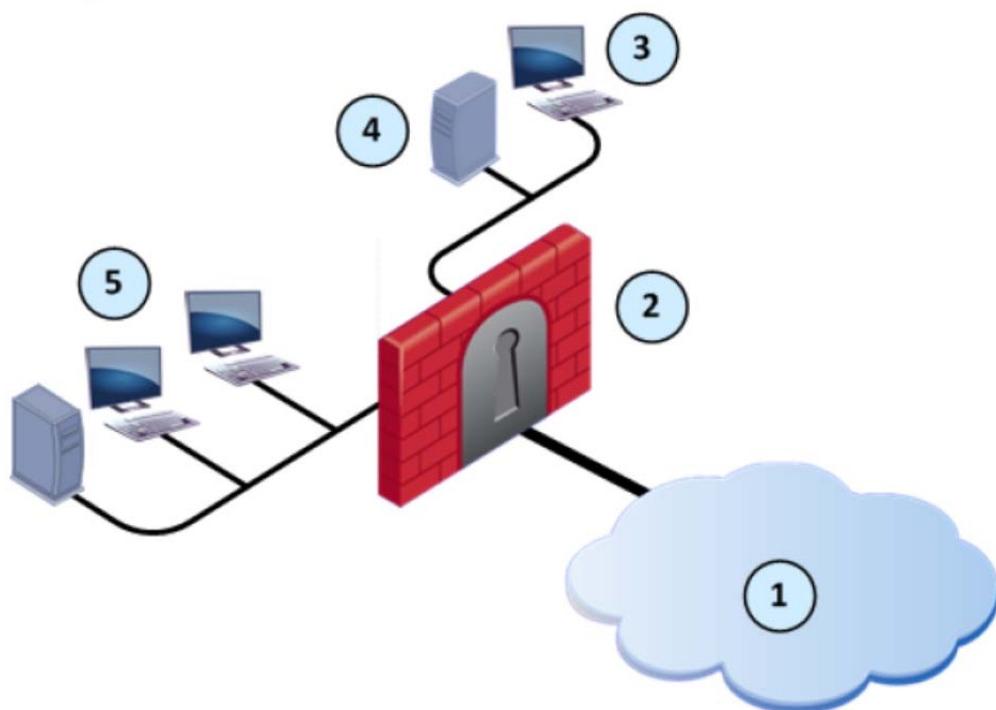


Exhibit 25.

1 95. For example, the '731 Accused Products include Next Generation Firewalls and
2 Security Gateways with security policies that serve as a collection of rules that control network traffic
3 and enforce organization guidelines for data protection and access to resources. The Next Generation
4 Firewalls and Security Gateways include the ThreatSpect Engine for multi-tiered analysis of network
5 traffic and correlation of data across multiple layers, including through antivirus, reputation, and
6 behavioral patterns.

Components of the Check Point Solution



20 | Exhibit 13 at Page 14.

21 96. For example, the '731 Accused Products include Smart-1 appliances for security
22 policy application and caching security policies.



27 | Exhibit 12 at Page 14.

1 97. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to
2 suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant both
3 compete in the security software space, as described above. And Finjan is actively engaged in
4 licensing its patent portfolio, as described. Check Point's continued infringement of the '731 Patent
5 causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of
6 business opportunities, inadequacy of money damages, and direct and indirect competition.
7 Monetary damages are insufficient to compensate Finjan for these harms. Accordingly, Finjan is
8 entitled to preliminary and/or permanent injunctive relief.

9 98. Defendant's infringement of the '731 Patent has injured Finjan in an amount to be
10 proven at trial.

11 99. Defendant has been long-aware of Finjan's patents, including the '731 Patent, and has
12 acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate,
13 wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of
14 its infringement of the '731 Patent. Defendant has had specific knowledge and notice of its
15 infringement of the '731 Patent since at least in or about December 2016, when Finjan specifically
16 identified and described the following products made, used, or sold by Defendants as infringing the
17 '731 Patent: Threat Prevention products, products with SandBlast zero-day protection, Next
18 Generation Firewall products, Web Security products, Mobile Security products, and Endpoint
19 Security products.

20 100. On information and belief, despite its knowledge of the '731 Patent and its knowledge
21 of its own infringement of that patent since at least in or about December 2016, Defendant made no
22 effort to design its products or services around the '731 Patent in order to avoid infringement.
23 Instead, on information and belief, Defendant incorporated infringing technology into additional
24 products, such as those identified in this Complaint. All of these actions demonstrate Defendant's
25 blatant and egregious disregard for Finjan's patent rights.

COUNT VI**(Indirect Infringement of the '731 Patent pursuant to 35 U.S.C. § 271(b))**

1 101. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
 2 allegations of the preceding paragraphs, as set forth above.

3 102. Defendant has induced and continues to induce infringement of one or more claims of
 4 the '731 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the '731 Patent,
 5 Defendant indirectly infringes the '731 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing
 6 and/or requiring others, including customers, purchasers, users and developers, to perform some of
 7 the steps of the method claims, either literally or under the doctrine of equivalents, of the '731 Patent,
 8 where all the steps of the method claims are performed by either Defendant or its customers,
 9 purchasers, users and developers, or some combination thereof. Defendant knew or was willfully
 10 blind to the fact that it was inducing others, including customers, purchasers, users and developers, to
 11 infringe by practicing, either themselves or in conjunction with Defendant, one or more method
 12 claims of the '731 Patent, including Claims 7-12, 14-16, and 20-21.

13 103. Defendant knowingly and actively aided and abetted the direct infringement of the '731
 14 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '731
 15 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third
 16 parties to use the '731 Accused Products in an infringing manner, providing a mechanism through
 17 which third parties may infringe the '731 Patent, advertising and promoting the use of the '731
 18 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties
 19 on how to use the '731 Accused Products in an infringing manner.

20 104. Defendant updates and maintains an website with Defendant's administration guides,
 21 user guides, operating instructions, and training and certifications which cover in depth aspects of
 22 operating the '731 Accused Products. *See, e.g.,*

23 <https://supportcenter.checkpoint.com/supportcenter/portal>, attached hereto as Exhibit 21.

COUNT VII**(Direct Infringement of the ‘633 Patent pursuant to 35 U.S.C. § 271(a))**

105. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
 3 allegations of the preceding paragraphs, as set forth above.

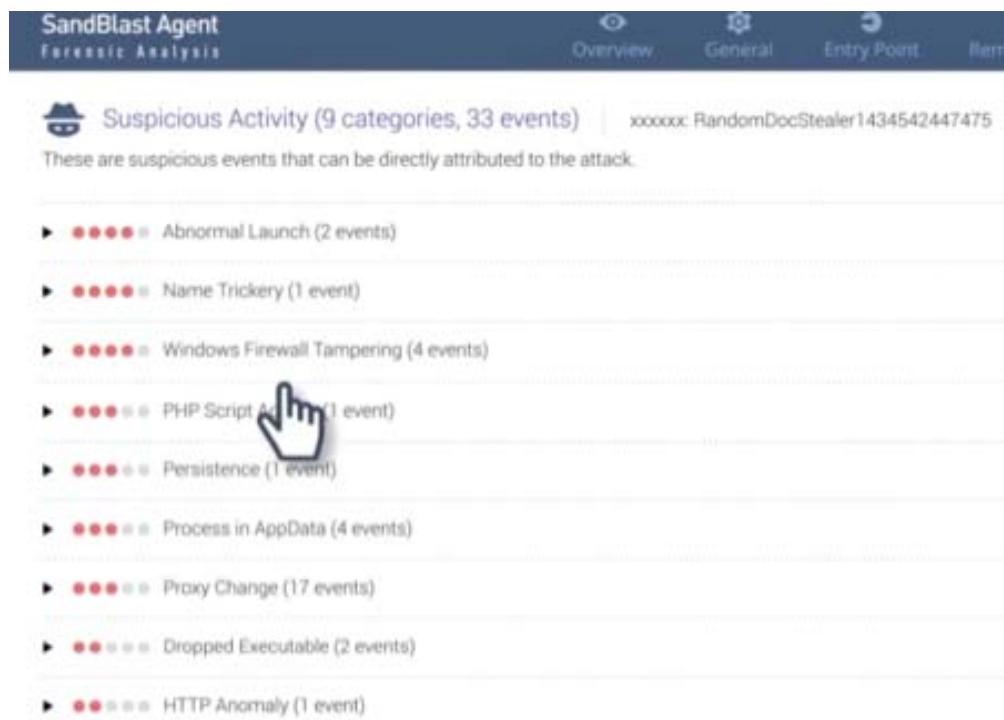
106. Defendant has infringed and continues to infringe Claims 1-45 of the ‘633 Patent in
 5 violation of 35 U.S.C. § 271(a). Defendant’s infringement is based upon literal infringement or
 6 infringement under the doctrine of equivalents, or both. Defendant’s acts of making, using, importing,
 7 selling, and/or offering for sale infringing products and services have been without the permission,
 8 consent, authorization, or license of Finjan. Defendant’s infringement includes the manufacture, use,
 9 sale, importation and/or offer for sale of Defendant’s products and services, including Check Point’s
 10 Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products,
 11 Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products,
 12 ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management
 13 products, ThreatCloud Managed Security Service products, Smart-1 Appliance products, products
 14 using SandBlast technology, and products utilizing the Gaia Operating System (collectively, the “‘633
 15 Accused Products”).

107. The ‘633 Accused Products embody the patented invention of the ‘633 Patent and
 17 infringe the ‘633 Patent because they perform the method of receiving, by a computer, downloadable-
 18 information; determining, by the computer, whether the downloadable-information includes
 19 executable code; and based upon the determination, transmitting from the computer mobile protection
 20 code to at least one information-destination of the downloadable-information, if the downloadable-
 21 information is determined to include executable code. *See generally* Exhibit 5.

108. For example, as shown below, the ‘633 Accused Products provide gateway security to
 23 end users, where incoming downloadable information (e.g., PDFs with JavaScript, EXE files, or
 24 JavaScript embedded within an HTML file) is received by the ‘633 Accused Products. The ‘633
 25 Accused Products include components for determining if this received downloadable information

1 includes executable code. If so, the ‘633 Accused Products transmit mobile protection code to
 2 emulation technology that uses an evasion resistant sandbox.

3 109. For example, the ‘633 Accused Products package downloadable content with mobile
 4 protection code and sends this information to be sandboxed at an endpoint. The mobile protection
 5 code records suspicious activity.

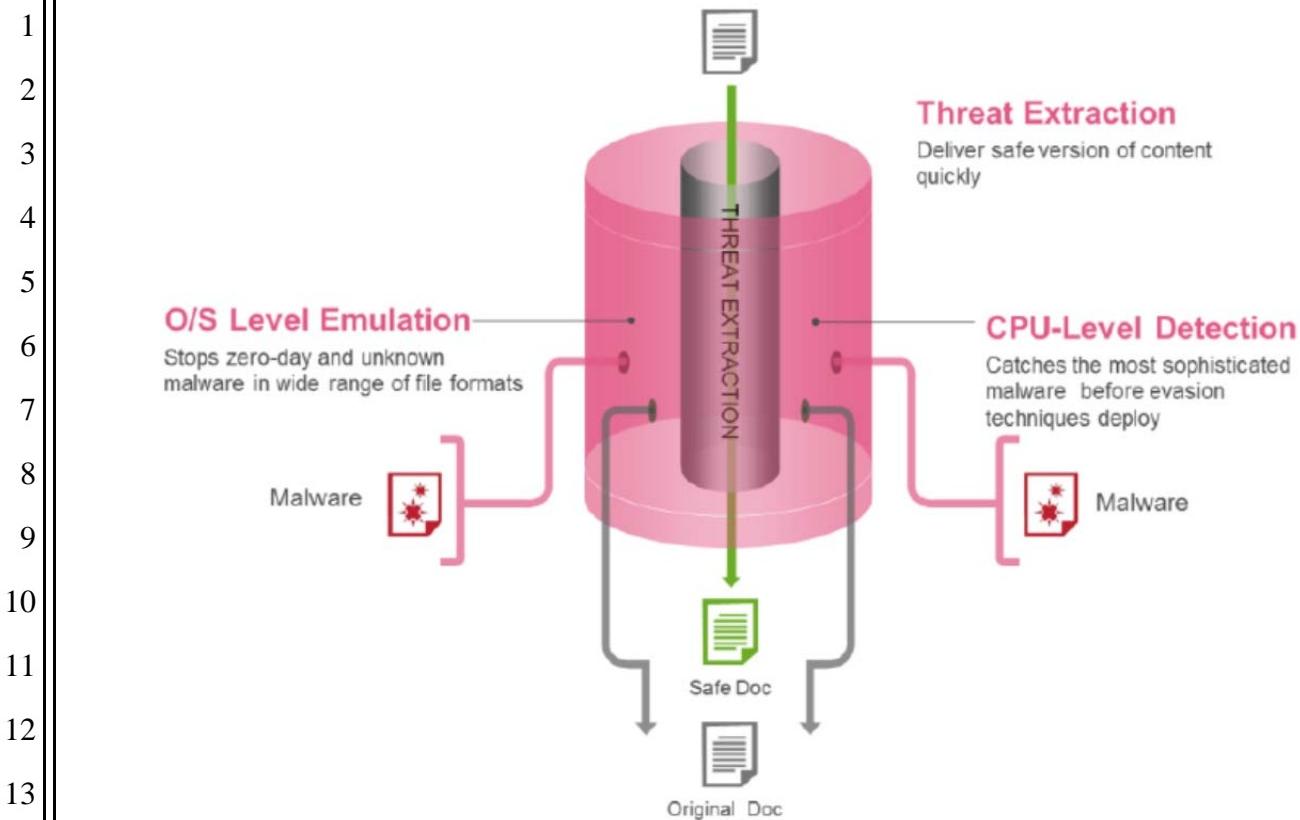


The screenshot shows the SandBlast Agent Forensic Analysis interface. At the top, there's a navigation bar with tabs: Overview, General, Entry Point, and Item. Below the navigation bar, the title "SandBlast Agent" and "Forensic Analysis" is displayed. A sub-section title "Suspicious Activity (9 categories, 33 events)" is shown, along with a note: "These are suspicious events that can be directly attributed to the attack." A large list of suspicious activity categories follows, each preceded by a small icon and a counter:

- ▶  Abnormal Launch (2 events)
- ▶  Name Trickery (1 event)
- ▶  Windows Firewall Tampering (4 events)
- ▶  PHP Script Analysis (1 event) 
- ▶  Persistence (1 event)
- ▶  Process in AppData (4 events)
- ▶  Proxy Change (17 events)
- ▶  Dropped Executable (2 events)
- ▶  HTTP Anomaly (1 event)

18 Exhibit 22.

19 110. For example, the ‘633 Accused Products infringe because they transmit downloadable
 20 information and mobile protection code to SandBlast Threat Emulation, which scans content and
 21 creates content profiles when it performs deep level inspection of downloaded content, both
 22 executables and data files, before the malware has a chance to deploy. SandBlast Threat Emulation
 23 runs files in a virtual sandbox to discover malicious behavior by monitoring the instructions
 24 performed and determining if the instruction relate to an exploit from malware. SandBlast Threat
 25 Emulation includes CPU-Level Inspection, which looks into the execution flow to determine if an
 26 exploitation method was used.



14 Exhibit 17 at 2 (August 2, 2016).

15 111. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to
16 suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant both
17 compete in the security software space, as described above. And Finjan is actively engaged in
18 licensing its patent portfolio, as described above. Check Point's continued infringement of the '633
19 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss
20 of business opportunities, inadequacy of money damages, and direct and indirect competition.
21 Monetary damages are insufficient to compensate Finjan for these harms. Accordingly, Finjan is
22 entitled to preliminary and/or permanent injunctive relief.

23 112. Defendant's infringement of the '633 Patent has injured Finjan in an amount to be
24 proven at trial.

25 113. Defendant has been long-aware of Finjan's patents, including the '633 Patent, and has
26 acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate,
27
28

1 wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of
2 its infringement of the ‘633 Patent. Defendant has had specific knowledge and notice of its
3 infringement of the ‘633 Patent since at least in or about December 2016, when Finjan specifically
4 identified and described the following products made, used, or sold by Defendants as infringing the
5 ‘633 Patent: Threat Prevention products, products with SandBlast zero-day protection, Next
6 Generation Firewall products, Web Security products, Mobile Security products, and Endpoint
7 Security products.

8 114. On information and belief, despite its knowledge of the ‘633 Patent and its knowledge
9 of its own infringement of that patent since at least in or about December 2016, Defendant made no
10 effort to design its products or services around the ‘633 Patent in order to avoid infringement.
11 Instead, on information and belief, Defendant incorporated infringing technology into additional
12 products, such as those identified in this Complaint. All of these actions demonstrate Defendant’s
13 blatant and egregious disregard for Finjan’s patent rights.

COUNT VIII

16 115. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
17 allegations of the preceding paragraphs, as set forth above.

18 116. Defendant has induced and continues to induce infringement of one or more claims of
19 the ‘633 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the ‘633 Patent,
20 Defendant indirectly infringes the ‘633 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing
21 and/or requiring others, including customers, purchasers, users and developers, to perform some of
22 the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘633 Patent,
23 where all the steps of the method claims are performed by either Defendant or its customers,
24 purchasers, users and developers, or some combination thereof. Defendant knew or was willfully
25 blind to the fact that it was inducing others, including customers, purchasers, users and developers, to
26 infringe by practicing, either themselves or in conjunction with Defendant, one or more claims of the
27 ‘633 Patent, including Claims 1-7 and 28-33.

117. Defendant knowingly and actively aided and abetted the direct infringement of the ‘633 Patent by instructing and encouraging its customers, purchasers, users and developers to use the ‘633 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third parties to use the ‘633 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘633 Patent, advertising and promoting the use of the ‘633 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘633 Accused Products in an infringing manner.

118. Defendant updates and maintains an website with Defendant's administration guides, user guides, operating instructions, and training and certifications which cover in depth aspects of operating the '633 Accused Products. *See, e.g.*,

<https://supportcenter.checkpoint.com/supportcenter/portal>, attached hereto as Exhibit 21.

COUNT IX

119. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

120. Defendant infringed Claims 1-42 of the ‘086 Patent in violation of 35 U.S.C. § 271(a). Defendant’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both. Defendant’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan. Defendant’s infringement includes the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including Check Point’s Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products, Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products, ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management products, ThreatCloud Managed Security Service products, Smart-1 Appliance products, products using SandBlast technology, and products utilizing the Gaia Operating System (collectively, the “‘086 Accused Products”).

1 121. The '086 Accused Products embody the patented invention of the '086 Patent and
 2 infringe the '086 Patent because they perform a method of receiving an incoming Downloadable;
 3 deriving security profile data for the Downloadable, including a list of suspicious computer
 4 operations that may be attempted by the Downloadable; appending a representation of the
 5 Downloadable security profile data to the Downloadable, to generate an appended Downloadable;
 6 and transmitting the appended Downloadable to a destination computer. *See generally* Exhibit 6.

7 122. For example, as shown below, the '086 Accused Products provide gateway security to
 8 end users, where incoming Downloadables (e.g., PDFs with JavaScript, EXE files, or JavaScript
 9 embedded within an HTML file) are received by the '086 Accused Products. For example, the '086
 10 Accused Products include emulation technology that uses an evasion resistant sandbox to catch
 11 unknown downloaded malware and eliminates threats and delivers safe files to users. The '086
 12 Accused Products create a profile with detailed information identifying suspicious code that was
 13 present in the content.

14 123. For example, the '086 Accused Products perform extensive forensics regarding the
 15 detected malware and associated events.

16 **Unified Malware and Bot Protection**

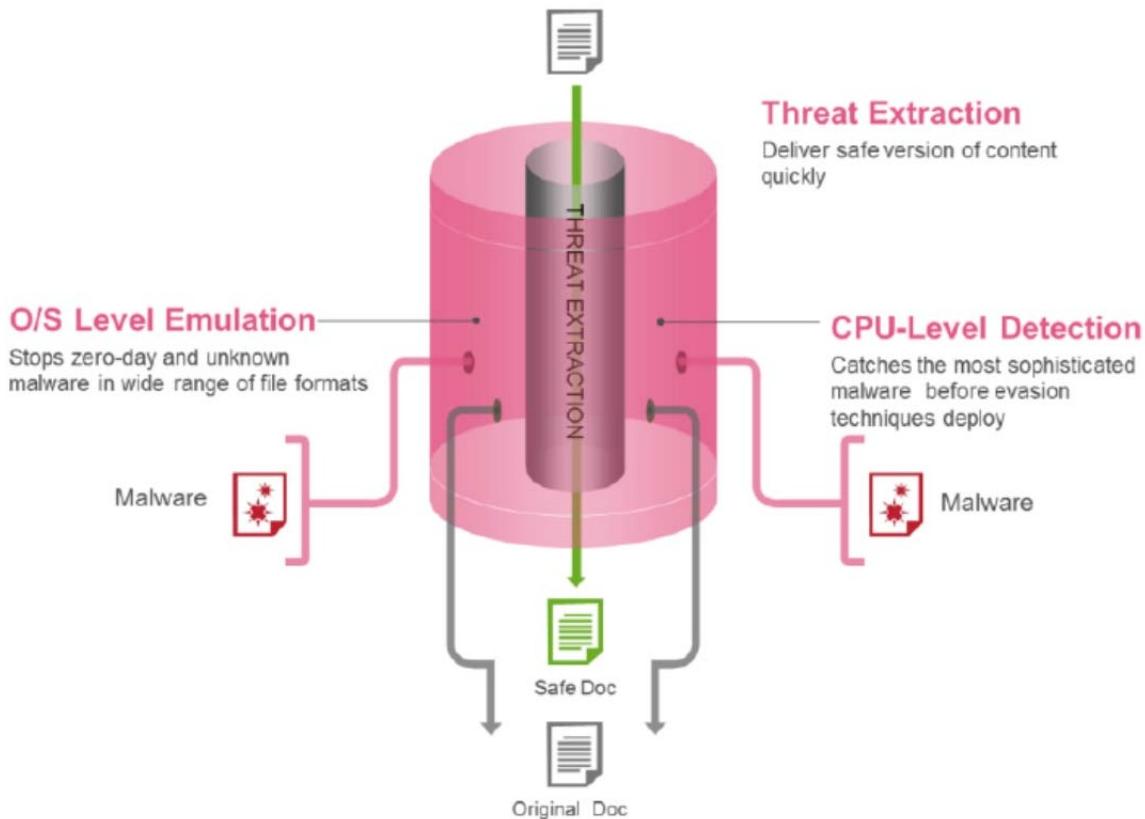
17 The Antivirus Software Blade is unified with the Anti-Bot
 18 Software Blade to give both pre-and post-infection protection
 19 to organizations and provide multi-layered threat prevention.
 Administrators can manage unified policies and reports all in
 a single user interface.



26 Extensive Forensics.

27 Exhibit 14 at Page 2.

124. For example, the '086 Accused Products include SandBlast Threat Emulation, which
 2 performs deep level inspection of downloaded content, both executables and data files, before the
 3 malware has a chance to deploy. SandBlast Threat Emulation runs files in a virtual sandbox to
 4 discover malicious behavior by monitoring the instructions performed, creating a profile, and
 5 determining if the instruction relate to an exploit from malware. SandBlast Threat Emulation
 6 includes CPU-Level Inspection, which looks into the execution flow to determine if an exploitation
 7 method was used. SandBlast Threat Emulation creates a detailed report for each file that is emulated
 8 and found to be malicious. SandBlast Threat Extraction extracts potentially malicious content, such
 9 as macros or embedded links, from files to allow prompt delivery of clean and reconstructed versions
 10 of these files that only include known safe elements. SandBlast sends the Downloadable and profile
 11 to other destinations to automatically share newly discovered attack information with ThreatCloud.



25 Exhibit 17 at 2 (August 2, 2016).
 26
 27
 28

125. For example, the ‘086 Accused Products sends profile information to be sandboxed at an endpoint. The mobile protection code records suspicious activity.

Suspicious Activity	(9 categories, 33 events)
	xxxxxx: RandomDocStealer1434542447475
These are suspicious events that can be directly attributed to the attack.	
▶	● ● ● ● Abnormal Launch (2 events)
▶	● ● ● ● Name Trickery (1 event)
▶	● ● ● ● Windows Firewall Tampering (4 events)
▶	● ● ● ● PHP Script Activity (1 event) 
▶	● ● ● ● Persistence (1 event)
▶	● ● ● ● Process in AppData (4 events)
▶	● ● ● ● Proxy Change (17 events)
▶	● ● ● ● Dropped Executable (2 events)
▶	● ● ● ● HTTP Anomaly (1 event)

Exhibit 22.

126. Defendant's infringement of the '086 Patent has injured Finjan in an amount to be proven at trial.

127. Defendant has been long-aware of Finjan’s patents, including the ‘086 Patent, and has acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the ‘086 Patent. Defendant has had specific knowledge and notice of its infringement of the ‘086 Patent since at least in or about December 2016, when Finjan specifically identified and described the following products made, used, or sold by Defendants as infringing the ‘086 Patent: Threat Prevention products, products with SandBlast zero-day protection, Next Generation Firewall products, Web Security products, Mobile Security products, and Endpoint Security products.

128. On information and belief, despite its knowledge of the ‘086 Patent and its knowledge of its own infringement of that patent since at least in or about December 2016, Defendant made no effort to design its products or services around the ‘086 Patent in order to avoid infringement. Instead, on information and belief, Defendant incorporated infringing technology into additional products, such as those identified in this Complaint. All of these actions demonstrate Defendant’s blatant and egregious disregard for Finjan’s patent rights.

COUNT X

129. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

130. Defendant induced infringement of one or more claims of the ‘086 Patent under 35 U.S.C. § 271(b). In addition to directly infringing the ‘086 Patent, Defendant indirectly infringes the ‘086 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘086 Patent, where all the steps of the method claims are performed by either Defendant or its customers, purchasers, users and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more claims of the ‘086 Patent, including Claims 1-8, 17-23, 31-32, 35-36, 39, and 41.

131. Defendant knowingly and actively aided and abetted the direct infringement of the ‘086 Patent by instructing and encouraging its customers, purchasers, users and developers to use the ‘086 Accused Products. Such instruction and encouragement includes, but is not limited to, advising third parties to use the ‘086 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘086 Patent, advertising and promoting the use of the ‘086 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘086 Accused Products in an infringing manner.

132. Defendant updates and maintains an website with Defendant's administration guides, user guides, operating instructions, and training and certifications which cover in depth aspects of operating the '086 Accused Products. *See, e.g.*,
<https://supportcenter.checkpoint.com/supportcenter/portal>, attached hereto as Exhibit 21.

COUNT XI

(Direct Infringement of the ‘154 Patent pursuant to 35 U.S.C. § 271(a))

133. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

134. Defendant has infringed and continues to infringe Claims 1-12 of the ‘154 Patent in violation of 35 U.S.C. § 271(a). Defendant’s infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents. Defendant acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan. Defendant’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including Check Point’s Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products, Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products, ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management products, ThreatCloud Managed Security Service products, Smart-1 Appliance products, products using SandBlast technology, and products utilizing the Gaia Operating System (collectively, the “‘154 Accused Products”).

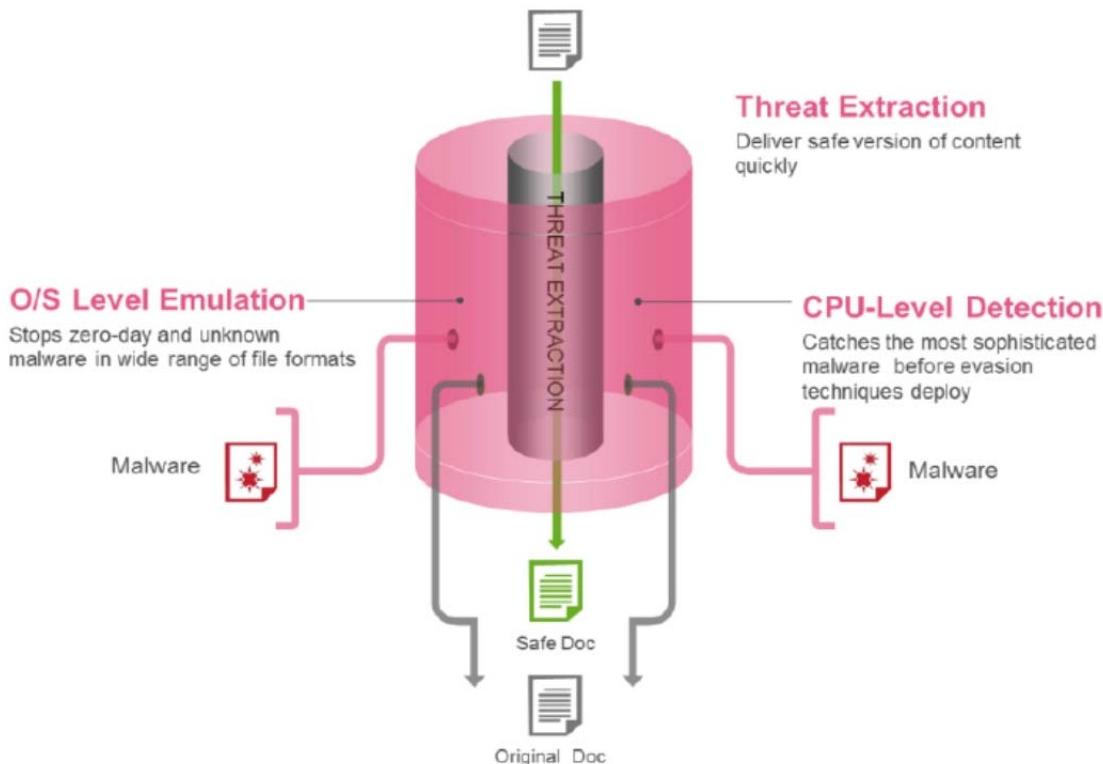
135. The ‘154 Accused Products embody the patented invention of the ‘154 Patent and infringe the ‘154 Patent because they utilize and/or incorporate a system for protecting a computer from dynamically generated malicious content, comprising: a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe; a transmitter for transmitting the input to the security computer for

1 inspection, when the first function is invoked; and a receiver for receiving an indication from the
 2 security computer whether it is safe to invoke the second function with the input.

3 136. For example, as shown below, the ‘154 Accused Products act as a content processor to
 4 process content or data received over the network, where that content includes a call to a first function
 5 that contains an input.

6 137. For example, ‘154 Accused Products transmit inputs that may invoke malicious actions
 7 to emulation technology that uses an evasion resistant sandbox to catch unknown downloaded malware
 8 and eliminates threats. The ‘154 Accused Products then deliver safe files to users.

9 138. For example, SandBlast Threat Emulation performs deep level inspection of
 10 downloaded content, both executables and data files, before the malware has a chance to deploy.
 11 SandBlast Threat Emulation transmits inputs to a virtual sandbox in the cloud or on another appliance
 12 to discover malicious behavior by monitoring the instructions performed and determining if the
 13 instruction relate to an exploit from malware. SandBlast automatically shares newly discovered
 14 attack information with ThreatCloud.



27 Exhibit 17 at 2 (August 2, 2016).

139. For example, ‘154 Accused Products prevent suspicious actions by evaluating an input using an endpoint agent.

Suspicious Activity (9 categories, 33 events)

These are suspicious events that can be directly attributed to the attack.

- ▶  Abnormal Launch (2 events)
- ▶  Name Trickery (1 event)
- ▶  Windows Firewall Tampering (4 events)
- ▶  PHP Script Attack (1 event)

- ▶  Persistence (1 event)
- ▶  Process in AppData (4 events)
- ▶  Proxy Change (17 events)
- ▶  Dropped Executable (2 events)
- ▶  HTTP Anomaly (1 event)

Exhibit 22.

140. For example, ‘154 Accused Products utilize Threat Cloud global security intelligence by submitting an input to the Threat Cloud to identify malware or a request to a command and control server.

141. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant both compete in the security software space, as described above. And Finjan is actively engaged in licensing its patent portfolio, as described above. Check Point's continued infringement of the '154 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

142. Defendant's infringement of the '154 Patent has injured and continues to injure Finjan
in an amount to be proven at trial.

143. Defendant has been long-aware of Finjan's patents, including the '154 Patent, and has acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '154 Patent.

144. On information and belief, despite its knowledge of the ‘154 Patent and its knowledge of its own infringement of that patent since at least on or about December 2016, Defendant made no effort to design its products or services around the ‘154 Patent in order to avoid infringement. Instead, on information and belief, Defendant incorporated infringing technology into additional products, such as those identified in this Complaint. All of these actions demonstrate Defendant’s blatant and egregious disregard for Finjan’s patent rights.

COUNT XII

(Direct Infringement of the ‘494 Patent pursuant to 35 U.S.C. § 271(a))

145. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

146. Defendant infringed Claims 3-5 and 7-18 of the ‘494 Patent in violation of 35 U.S.C. § 271(a). Defendant’s infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents. Defendant acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan. Defendant’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant’s products and services, including its Check Point’s Next Generation Firewall and Security Gateway products, Blade products, CloudGuard products, Endpoint Protection products, Advanced Threat Prevention products, Mobile Security products, ZoneAlarm products, Threat Intelligence products, Security Management and Policy Management products, ThreatCloud Managed Security Service products, Smart-1

1 Appliance products, products using SandBlast technology, and products utilizing the Gaia Operating
2 System (collectively, the ““494 Accused Products”).

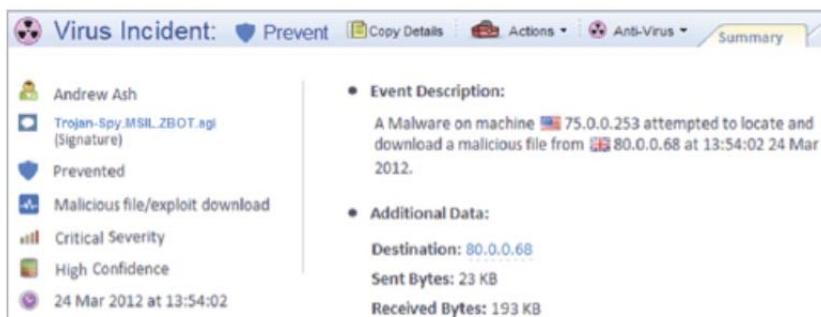
3 147. The ‘494 Accused Products embody the patented invention of the ‘494 Patent and
4 infringe the ‘494 Patent because they practice a computer-based method comprised of receiving an
5 incoming downloadable, deriving security profile data for the downloadable, including a list of
6 suspicious computer operations that may be attempted by the downloadable, and storing the
7 downloadable security profile data in a database. For example, as shown below, the ‘494 Accused
8 Products provide security to end users, where incoming downloadables are received by the ‘494
9 Accused Products.

10 148. For example, ‘494 Accused Products include emulation technology that uses an evasion
11 resistant sandbox to catch unknown downloaded malware and eliminates threats and delivers safe files
12 to users. The ‘494 Accused Products create a report with detailed information identifying suspicious
13 operations that the content may perform. The ‘494 Accused Products store the results in a database for
14 future use and retrieval.

149. For example, '494 Accused Products perform extensive forensics regarding the
detected malware and associated events and stores the results in a database.

Unified Malware and Bot Protection

The Antivirus Software Blade is unified with the Anti-Bot Software Blade to give both pre-and post-infection protection to organizations and provide multi-layered threat prevention. Administrators can manage unified policies and reports all in a single user interface.



Extensive Forensics.

Exhibit 14 at Page 2.

1 150. For example, SandBlast Threat Emulation performs deep level inspection of
 2 downloaded content, both executables and data files, before the malware has a chance to deploy.
 3 SandBlast Threat Emulation runs files in a virtual sandbox to discover malicious behavior by
 4 monitoring the instructions performed and determining if the instruction relate to an exploit from
 5 malware. SandBlast Threat Emulation includes CPU-Level Inspection, which looks into the
 6 execution flow to determine if an exploitation method was used. SandBlast Threat Emulation creates
 7 a detailed report for each file that is emulated and includes suspicious operations identified.
 8 SandBlast Threat Emulation stores the results in a database for future use and retrieval. SandBlast
 9 Threat Extraction extracts potentially malicious content, such as macros or embedded links, from files
 10 to allow prompt delivery of clean and reconstructed versions of these files that only include known
 11 safe elements. SandBlast automatically shares newly discovered attack information with
 12 ThreatCloud, which stores the results in a database.

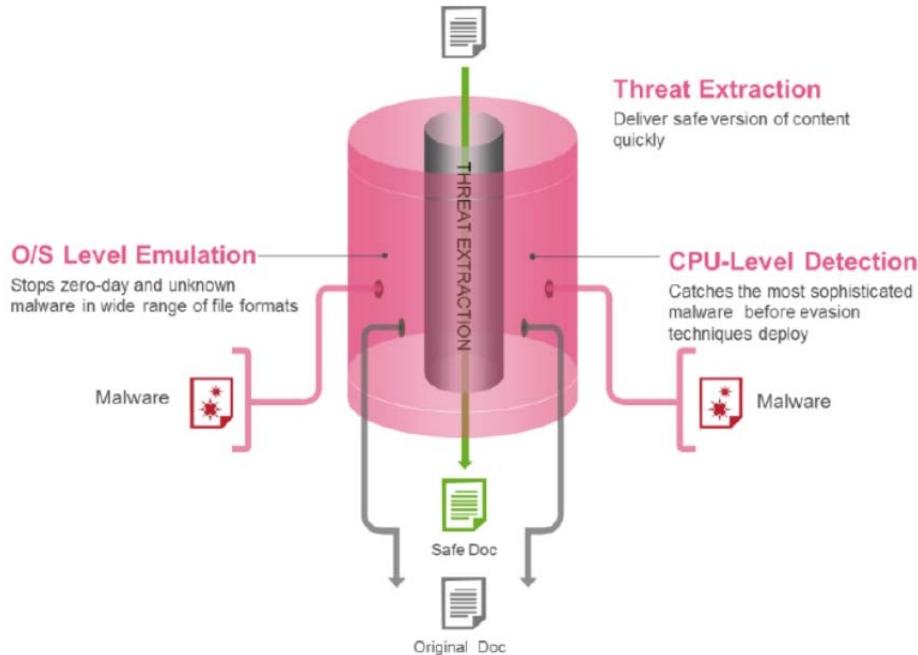


Exhibit 17 at 2 (August 2, 2016).

151. For example, suspicious activity is recorded about suspicious code that is detected.

Suspicious Activity (9 categories, 33 events) | x00000: RandomDocStealer14345424474745

These are suspicious events that can be directly attributed to the attack.

- ▶ Abnormal Launch (2 events)
- ▶ Name Trickery (1 event)
- ▶ Windows Firewall Tampering (4 events)
- ▶ PHP Script Ad (1 event)

- ▶ Persistence (1 event)
- ▶ Process in AppData (4 events)
- ▶ Proxy Change (17 events)
- ▶ Dropped Executable (2 events)
- ▶ HTTP Anomaly (1 event)

Exhibit 22.

152. Defendant's infringement of the '494 Patent has injured Finjan in an amount to be proven at trial.

153. Defendant has been long-aware of Finjan's patents, including the '494 Patent, and has acted recklessly and egregiously with conduct that is wanton, malicious, bad-faith, deliberate, wrongful, and flagrant by its continued infringing activity despite possessing specific knowledge of its infringement of the '494 Patent. Defendant has had specific knowledge of its infringement of the '494 Patent since at least in or about December 2016, when Finjan specifically identified and described the following products made, used, or sold by Defendants as infringing the '494 Patent: products with Threat Prevention Products, products with SandBlast zero-day protection, Next Generation Firewall products, Web Security products, Mobile Security products, and Endpoint Security products.

154. On information and belief, despite its knowledge of the ‘494 Patent and its knowledge of its own infringement of that patent since at least in or about December 2016, Defendant made no effort to design its products or services around the ‘494 Patent in order to avoid infringement.

1 Instead, on information and belief, Defendant incorporated infringing technology into additional
 2 products, such as those identified in this Complaint. All of these actions demonstrate Defendant's
 3 blatant and egregious disregard for Finjan's patent rights.

4 **COUNT XIII**

5 **(Indirect Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(b))**

6 155. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
 7 allegations of the preceding paragraphs, as set forth above.

8 156. Defendant induced infringement of at least Claims 3-5 and 7-9 of the '494 Patent
 9 under 35 U.S.C. § 271(b). In addition to directly infringing the '494 Patent, Defendant indirectly
 10 infringes the '494 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring
 11 others, including customers, purchasers, users and developers, to perform one or more of the steps of
 12 the method claims, either literally or under the doctrine of equivalents, of the '494 Patent, where all
 13 the steps of the method claims are performed by either Defendant, its customers, purchasers, users,
 14 and developers, or some combination thereof. Defendant knew or was willfully blind to the fact that
 15 it was inducing others, including customers, purchasers, users, and developers, to infringe by
 16 practicing, either themselves or in conjunction with Defendant, one or more method claims of the
 17 '494 Patent, including Claims 3-5 and 7-9.

18 157. Defendant knowingly and actively aided and abetted the direct infringement of the
 19 '494 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the
 20 '494 Accused Products. Such instruction and encouragement includes, but is not limited to, advising
 21 third parties to use the '494 Accused Products in an infringing manner, providing a mechanism
 22 through which third parties may infringe the '494 Patent, advertising and promoting the use of the
 23 '494 Accused Products in an infringing manner, and distributing guidelines and instructions to third
 24 parties on how to use the '494 Accused Products in an infringing manner.

25 158. Defendant updates and maintains a website with Defendant's administration guides,
 26 user guides, operating instructions, and training and certifications which cover in depth aspects of

1 operating the '494 Accused Products. *See, e.g.*,

2 <https://supportcenter.checkpoint.com/supportcenter/portal>, attached hereto as Exhibit 21.

3 **PRAYER FOR RELIEF**

4 WHEREFORE, Finjan prays for judgment and relief as follows:

5 A. An entry of judgment holding that Check Point has infringed the '844 Patent, the '968
 6 Patent, the '731 Patent, the '633 Patent, the '086 Patent, the '154 Patent, and the '494 Patent, and is
 7 continuing to infringe the '968 Patent, the '731 Patent, the '633 Patent, and the '154 Patent; and has
 8 induced infringement of the '844 Patent, the '968 Patent, the '731 Patent, the '633 Patent, the '086
 9 Patent, and the '494 Patent;

10 B. A preliminary and permanent injunction against Check Point and its officers,
 11 employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from
 12 continuing to infringe the '968 Patent, the '731 Patent, the '633 Patent, and the '154 Patent, and for
 13 all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

14 C. An award to Finjan of such past damages as it shall prove at trial against Check Point
 15 that are adequate to fully compensate Finjan for Check Point's infringement of the '844 Patent, the
 16 '968 Patent, the '731 Patent, the '633 Patent, the '086 Patent, '154 Patent, and the '494 Patent, said
 17 damages to be no less than a reasonable royalty;

18 D. A finding that this case is "exceptional" and an award to Finjan of its costs and
 19 reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

20 E. An accounting of all infringing sales and revenues, together with post judgment
 21 interest and prejudgment interest from the first date of infringement of the '844 Patent, the '968
 22 Patent, the '731 Patent, the '633 Patent, the '086 Patent, '154 Patent, and the '494 Patent; and

23 F. Such further and other relief as the Court may deem proper.

1
2 Dated: May 3, 2018
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Respectfully submitted,

By: /s/ Paul J. Andre

Paul J. Andre (State Bar No. 196585)

Lisa Kobialka (State Bar No. 191404)

James Hannah (State Bar No. 237978)

Austin Manes (State Bar No. 284065)

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

990 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 752-1700

Facsimile: (650) 752-1800

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

amanes@kramerlevin.com

12 *Attorneys for Plaintiff*

13 FINJAN, INC.

1 **DEMAND FOR JURY TRIAL**

2 Finjan demands a jury trial on all issues so triable.

3 Respectfully submitted,

4 Dated: May 3, 2018

By: /s/ Paul J. Andre

5 Paul J. Andre (State Bar No. 196585)

6 Lisa Kobialka (State Bar No. 191404)

7 James Hannah (State Bar No. 237978)

Austin Manes (State Bar No. 284065)

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

9 990 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 752-1700

Facsimile: (650) 752-1800

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

amanes@kramerlevin.com

13 *Attorneys for Plaintiff*

14 FINJAN, INC.